Pairing computation and arithmetic of elliptic curves for cryptography

Emmanuel Fouotsa

THÈSE / UNIVERSITÉ DE RENNES 1
sous le sceau de l'Université Européenne de Bretagne

pour le grade de

DOCTEUR DE L'UNIVERSITÉ DE RENNES 1

Mention : Mathématiques et Applications

Ecole doctorale MATISSE

Présentée par

Emmanuel FOUOTSA

Préparée à l'unité de recherche
6625 CNRS - IRMAR
Institut de Recherche de Mathématiques de Rennes
U.F.R. de Mathématiques

Calcul des Couplages et Arithmétique des Courbes Elliptiques pour la Cryptographie

Thèse soutenue à Rennes
le 02 Décembre 2013

devant le jury composé de :

Christophe RITZENTHALER
Professeur, Université de Rennes 1 (France) / *Président*

Jean-Marc COUVEIGNES
Professeur, Université de Bordeaux 1 (France) / *rapporteur*

Djiby SOW
Professeur, Université Cheik Anta Diop de Dakar (Sénégal) / *rapporteur*

Tony EZOME
Maître Assistant CAMES, Université des Sciences et Techniques de Masuku, Franceville (Gabon) / *examinateur*

Sylvain DUQUESNE
Professeur, Université de Rennes 1 (France) / *directeur de thèse*

Dédicace

To
my daughter ***Grace Divine***,
and
her mother, my beloved wife ***Edith***,
For their love and support.

Remerciements

This thesis was carried out in co-supervision in the laboratory IRMAR, University of Rennes 1 (France) and in the Department of Mathematics of the University of Yaounde 1 (Cameroon). I would like to begin by expressing my gratitude to my jury's members :

I would like to thank Professors **Jean-Marc Couveignes** and **Djiby Sow** who accepted to be reviewers for this work. Thanks also to Professor **Christophe Ritzenthaler** to have accepted to be the president of the jury and Professor **Tony Ezome** who accepted to be the examiner in my jury.

I am deeply grateful to Professor **Sylvain Duquesne** for the research topic on which we have worked. I thank him for letting me the freedom to express myself in all our exchanges during these past years. This has been very supportive to me for this work. In addition he has played a fundamental role in various applications for funding that I submitted for stays of research and participation to conferences and schools related to my research topic. From his inspirational support and criticism, I learned a lot about doing research and presenting it. Always available to answer my many questions and really determined to a good education to scientific research. I will remain forever grateful.

I would also like to extend my deepest gratitude to Professor **Marcel Tonga**, who believed in my skills and my desire to complete doctoral studies in cryptography. To this end, it has to be a solid bridge between me and Professor Sylvain Duquesne at the beginning and during the course of this thesis. I was deeply encouraged by listening and criticisms during my many presentations at ERAL (Research Team on Algebra and Logic), the research team that he was directed these past years. I take this opportunity to express my gratitude to some of the team members : **Dr. Nkuimi, Dr. Lele, Dr Nguefack, Dr. Nkianpi, Dr. Koguep, Dr. Temgoua** and **Dr. Fomekong**. They were particularly attentive to my talks for this new topic in the laboratory and they directed me deep encouragements.

I will never forget Professor **Daniel Tieudjo**. He believed in me and supported my work

in cryptography ever since the beginning. His relevant remarks about my earlier work on the applications of braid groups in cryptography gave me an enormous boost to help me move forward. I'm also very excited and grateful for his remarks.

Throughout the realization of this thesis, many research trips ought to be done. I had the opportunity to meet **Dr. Oumar Diao** at IRMAR. Oumar is a remarkable person. I owe him a lot for his support. Learning Sage and Magma softwares for the implementation of my research results. His work on theta functions interested me and marked the start of a series of collaborations between us. I am grateful for having agreed to make an article about this with me. Sometimes even distance has not prevented us to discuss by the phone or to exchange emails with long mathematical formulas. Oumar, thank you for that and for our prospects for future collaborations.

I am also very grateful to **Dr. Nadia El Mrabet** who invited me to LIASD (Laboratoire d'Informatique Advancée de Saint-Denis), Université Paris 8. She shared with me some of her expert knowledge about pairings computation. I'm glad to have an article with her and prospects for future collaborations. I remind and thank you for the "spicy meal" of an Indian restaurant you invited me in Paris !!.

I am deeply sensitive to the support that Professor **Marie Françoise Roy**, via the CIMPA (Centre Internationale de Mathématiques Pures et Appliquées) and the SARIMA (Soutient aux Activitées de Recherche en Informatique Mathématiques en Afrique), brought to me for the realisation of this thesis. Then responsible of CIMPA in sub-Saharan Africa, she generously provided the financial support through these organizations allowing me to attend many international conferences and research trips. These acknowledgments also extend to the laboratory IRMAR (Institut de Recherche Mathématiques de Rennes), University of Rennes, which has welcomed me several times during these past years. I want to also take this opportunity to express my gratitude to the Director of this Institute, **Bachir Bekka** and his adminsitrative team for giving me many pleasant stays in Rennes.

I am also indebted to a particular brother, **Dr Wotchoko** and colleagues in the department of mathematics at the Ecole Normale Supérieure, University of Bamenda. Particularly to Dr. **Akongnwiu Clement**, **Fomatati yves**, and my head of department, **Kum Cletus Nkwa**, for their support and understanding in my many shortcomings.

I have a deep gratitude towards my friends of "**CAS**", my brothers and friends **Ango Lotin**

and **Cyrille Simeu** who have supported me during these recent years. Thank you for letting me stay with you several times in Yaoundé. Thank you for your permanent encouragement Cyrille. You remain a good friend since we met in Master.

Thank you to **Nestor Folifack, Nicolas Kamdem, Cyrille Nganteu, Emmanuel Pola, Serge Tebu, Cyprien Wamnené** and **Hyacinthe Sonméné** for their prayers and permanent encouragements.

I am grateful to my wonderful **family inlaw**, for their moral support and encouragement. Their softness, love and prayers have been very supportive to me in recent years.

My family, the corner stone, is the place where I always resource. For their deep support, their permanent encouragement and their prayers every day, that they rejoice of this work themselves that demonstrates the greatness of their support. I am grateful to my beloved mom **Ngoumtsop Marie** for her love. I remember with love, the encouraging words of his beloved husband, my late father **Kuete Pierre**

Kag tʉ mbonɔ́, ta ngwɔ ngẅiin paga ŋwà'ne gie mé toŋo ngie DEA la,
mba menod mú kwă' ngyɔɔn, pu'u la ɔ ku' pa' ɔ ge pɔɔnte,
ŋwe'e maama lepu'u ŋwà'ne lelɔg nkẅe Doktola.

Although he is no longer alive, these words comforted me a lot during this work.

I would like to give a special thanks to my dear wife **Edith Akenné** for her undying love, enormous support and great patience. With her endless understanding and generous encouragement, I have been able to do this thesis and my professionnal duty in a sweet and peaceful environment.

Table des matières

Liste des abbréviations

Dans cette thèse nous utilisons les notations suivantes :

p :	Entier premier
$\mathbb{F}_p$:	Corps fini de p élements
$\mathbb{K} := \mathbb{F}_q$:	Corps fini de q éléments où q est une puissance de l'entier p
$E(\mathbb{K})$:	Ensemble des points rationels de la courbe elliptique E défini sur le corps $\mathbb{K}$
P_0 :	Element neutre pour la loi de groupe dans $E(\mathbb{K})$
s_n :	Coût d'une élévation au carré dans le corps $\mathbb{F}_{q^n}$ où n est un entier naturel
m_n :	Coût d'une multiplication dans le corps $\mathbb{F}_{q^n}$ où n est un entier naturel
mc :	Coût d'une multiplication par une constante dans le corps $\mathbb{F}_q$

Résumé en français

Cryptographie basée sur les courbes elliptiques (ECC) et les couplages

La cryptographie est l'étude des méthodes de chiffrement et de déchiffrement de l'information de telle sorte que seuls les utilisateurs autorisés peuvent déchiffrer et lire l'information originale. La cryptographie moderne est divisée en deux grandes parties : la cryptographie symétrique et la cryptographie à clé publique. Pour la cryptographie symétrique, la clé de déchiffrement peut se déduire facilement de la clé de chiffrement, tandis qu'en cryptographie à clé publique encore appelée cryptographie assymmétrique, la clé de déchiffrement est difficilement calculable à partir de la clé de chiffrement. Dans ce dernier cas, les deux clés sont liées par une fonction à sens unique. Cette difficulté est donc en général liée à l'impossibilité de résoudre en temps polynomiale des problèmes mathématiques tels que la factorisation des grands nombres composés ou le calcul du logarithme discret dans un groupe. Jusqu'à il y a quelques années, le crypto système le plus utilisé est le crypto système RSA inventé par **R**ivest, **S**hamir and **A**delmann [66]. Sa sécurité est justement basée sur le problème de la factorisation d'un grand entier composé, de l'ordre de 1024 bits. De nos jours, le meilleur algorithme qui résout ce problème est le Crible Quadratique des Nombres avec une complexité déjà sous exponentielle [44, Chapter 3]. Cette complexité est telle que pour un niveau de sécurité de 80 bits dans un tel crypto système, on doit effectuer des opérations modulo 1024, ce qui implique d'utiliser des nombres de tailles raisonnablement élevées pour des hauts niveaux de sécurité. Ce qui est déjà un désavantage pour RSA pour les nouveaux besoins en peu de ressources des applications du millénaire telles que les cartes à puces, les dispositifs à puissances limitée dans des serveurs web, qui ont besoin d'effectuer rapidement des millions de transactions sécurisées pour la banque et le commerce en ligne par exemple. De même, ce problème d'efficacité dans les calculs demeure aussi même si on considère la cryptographie à clé publique basée sur le Logarithme Discret dans les corps finis. En effet, le Calcul d'indice résout aussi ce problème avec une complexité sous exponentielle [44, Chapter 2]. Face à cette situation, la communauté scientifique est de plus en plus intéressée par la cryptographie basée sur les courbes elliptiques car celle ci offre

une efficacité inégalée pour les calculs et ceci à un niveau de sécurité égal avec RSA.
La cryptographie basée sur les courbes elliptiques tire son origine des travaux de Miller [59] et Koblitz [48] qui ont suggérés d'utiliser la difficulté de résoudre le problème du logarithme discret dans le groupe de points rationnels d'une courbe elliptique pour faire la cryptographie. Dans ce groupe $E(\mathbb{F}_q)$, le logarithme discret est défini comme suit : Etant donné un couple de points $(P, Q = kP) \in E(\mathbb{F}_q)^2$, déterminer l'entier $k \in [1, \sharp E(\mathbb{F}_q)[$, où $kP = P + P + ... + P$, $k-$ fois. Aucune attaque sous exponentielle n'est connue existée pour ce groupe en général. Par conséquent les longueurs des clés sont petites contrairement au cas des clés RSA comme le montre la Table 0.1.

TABLE 0.1 – Paramètres RSA et ECC

Niveau de sécurité en bits	80	112	128	192	256
Modules RSA en bits	1024	2048	3072	8192	15360
ECC : Taille du corps de base en bits	160	224	256	384	512

Pour cette raison, la cryptographie basée sur les courbes elliptiques se développe de plus en plus et beaucoup de protocoles sont standardisés par ISO (International Organisation for Standardisation) et NIST (National Institute of Standards and Technology). On peut consulter [38, Appendix B] pour plus de détails. Parmi les applications des courbes elliptiques en cryptographie, on note certaines, pas des moindres, offertes par des applications bilinéaires définies sur le groupe de points d'une courbe elliptique. Ces applications s'appellent couplages ou *pairings* en anglais.
Ce sont des outils mathématiques introduits par Weil en 1948 [78]. Soient $\mathbb{G}_1$ et $\mathbb{G}_2$ deux groupes abéliens finis notés additivement et d'élément neutre O. Supposons que $\mathbb{G}_1$ et $\mathbb{G}_2$ ont pour ordre n. Soit $\mathbb{G}_3$ un autre groupe multiplicatif cyclique d'ordre n et d'élément neutre 1. *Un couplage est une application*

$$e_n : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$$

qui satisfait les conditions suivantes :

- e_n *est bilinéaire :* $e_n(S_1+S_2, T) = e_n(S_1, T)e_n(S_2, T)$ *et* $e_n(S, T_1+T_2) = e_n(S, T_1)e_n(S, T_2)$ *Pour tout* S, S_1, $S_2 \in \mathbb{G}_1$ *et pour tout* T, T_1, $T_2 \in \mathbb{G}_2$.
- e_n *est non dégénéré : Pour tout* $P \in \mathbb{G}_1$, $P \neq O$, *il existe* $Q \in \mathbb{G}_2$ *tel que* $e_n(P, Q) \neq 1$. *Et pour tout* $Q \in \mathbb{G}_2$,$Q \neq O$ *il existe* $P \in \mathbb{G}_1$ *tel que* $e_n(P, Q) \neq 1$.

Les couplages ont été introduits en cryptographie pour la première fois par Menezes, Okamoto et Vanstone (MOV) [55] en 1993 et par Frey et Rück [57] en 1994 pour résoudre les instances du logarithme discret dans le groupe $E(\mathbb{F}_q)$ en utilisant respectivement les couplages de Weil et de Tate. Leur algorithme illustré dans la Table 0.2, utilise la bilinéarité des couplages pour

transférer le logarithme discret du groupe $E(\mathbb{F}_q)$ vers le logarithme discret dans les corps finis où il existe des algorithmes à complexité sous exponentielle [44].

TABLE 0.2 – Attaque MOV/Frey-Rück

Entrée : $P, Q \in E(\mathbb{F}_q)$, d'ordre premier r tels $Q = \lambda P$ pour un entier inconnu λ **Sortie :** Logarithme discret λ de Q en base P
1. Construire le corps $\mathbb{F}_{q^k}$ tel que r divise $(q^k - 1)$ 2. Trouver le point $S \in E(\mathbb{F}_{q^k})$ tel que $e_r(P, S) \neq 1$ 3. $\alpha_1 \longleftarrow e_r(P, S)$ 4. $\alpha_2 \longleftarrow e_r(Q, S)$ 5. Trouver λ tel que $\alpha_1^\lambda = \alpha_2$ dans $\mathbb{F}_{q^k}^\star$ en utilisant le calcul d'indice 6. Retourner λ.

La première utilisation des couplages était donc destructrice. Cependant les couplages sont très à la mode en cryptographie ces années car ils permettent de construire de nouveaux protocoles cryptographiques grâce à la difficulté calculatoire de certains problèmes tels que :

***Diffie Hellman Calculatoire Bilinéaire* (BDH) :** Etant donnés P, Q, $P_1 = aP$ et $P_2 = bP$ tels que $e(P, Q) \neq 1$, calculer $e(abP, Q)$.

***Diffie Hellman Décisionnel Bilinéaire* (DBDH) :** Etant donnés P, Q tels que $e(P, Q) \neq 1$, et $P_1 = aP$, $P_2 = bP$ et g. Tester si $g = e(abP, Q)$ ou pas.

Nous présentons ci-dessous deux exemples de base pour illustrer l'application des couplages en cryptographie.

Chiffrement à base d'identité de Boneh-Franklin.

Initialement suggeré par Shamir [69] en 1984, le chiffrement à base d'identité suppose qu'un chiffrement à clé publique peut être mis en œuvre avec l'identité du destinataire, ceci facilite alors la gestion des clés et des certificats. En effet, la clé publique du destinataire n'est pas calculée à l'avance et ne l'est qu'avec la seule identité de celui ci. Le chiffrement à base d'identité le plus connu fut proposé par Boneh et al. dans [11] en 2001 et est décrit comme suit :
Une autorité de confiance (AC) publie les paramètres $(\mathbb{G}_1, \mathbb{G}_3, e, P, Q_0, H_1, H_2)$ où $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_3$ est un couplage, la clé publique P est un générateur de $\mathbb{G}_1$. Le point $Q_0 = sP$ où $s \in \mathbb{Z}_n^\star$ est la clé privée de l'AC. $H_1 : \{0,1\}^* \to \mathbb{G}_1$ et $H_2 : \mathbb{G}_3 \to \{0,1\}^n$ sont deux fonctions cryptographiques

de hachages. Dans ce schéma, chaque identité X avec identité notée Id_X, recevra une clé privée $S_X = sQ_X$ où $Q_X = H_1(Id_X) \in G_1$ à travers un canal sécurisé. Supposons que Bob (B) veut envoyer un message clair $M \in \{0,1\}^n$ de n bits à Alice (A).

- B calcule $Q_A = H_1(Id_A)$
- B choisi $t < n$ au hasard
- B calcule le texte chiffré $C = [U = tP, V = M \oplus H_2(e(Q_A, Q_0))^t]$ et envoi à Alice.

Alice reçoit $C = [U, V]$ et peut retrouver le message M comme suit $M = V \oplus H_2(e(S_A, U))$. Pour observer comme la bilinéarité du couplage est utilisée pour le déchiffrement, observons que

$$e(Q_A, Q_0)^t = e(Q_A, P)^{st} = e(sQ_A, tP) = e(S_A, U)$$

Le calcul du masque de chiffrement $H_2(e(Q_A, Q_0)^t) = H_2(e(sQ_A, U))$ par un espion exige le calcul de $e(Q_A, Q_0)^t$ à partir de P, Q_A, Q_0 et $U = tP$. Ceci est clairement lié à la résolution du problème BDH.

Protocole d'échange de clé à trois parties.

Supposons que trois personnes Alice, Bob, et Carl veulent s'entendre sur une clé commune en utilisant une seule passe d'information entre deux personnes. Ceci est possible en utilisant la construction de Antoine Joux [47]. Nous donnons dans la Table 0.3 une description simple de cet algorithme. Soit P un générateur de $\mathbb{G}_1$ et Q un générateur de $\mathbb{G}_2$.

TABLE 0.3 – Protocole d'échange de clé à trois parties de Joux

Entrée : Paramètres publiques P, Q, $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_3$, un couplage e. **Sortie :** La clé commune $K \in \mathbb{G}_3$ pour Alice, Bob et Carl
1. Alice choisi un entier (sa clé privée) a calcule $P_a = aP$ et $Q_a = aQ$ puis envoie à Bob et Carl 2. Bob choisi un entier (sa clé privée) b calcule $P_b = bP$ et $Q_b = bQ$ puis envoie à Alice et Carl 3. Carl choisi un entier (sa clé privée) c calcule $P_c = cP$ et $Q_c = cQ$ puis envoie à Alice et Bob 4. La clé commune est : $K = e(P_b, Q_c)^a = e(P_a, Q_c)^b = e(P_a, Q_b)^c = e(P, Q)^{abc}$

Les protocoles de Joux et de Boneh-Franklin's sont d'importantes applications des couplages parmi tant d'autre à savoir :

- Le chiffrement basé sur l'identité de Cocks [16]

- Distribution non interactive de clé basée sur l'identité [68]
- Signatures indéniables basées sur l'identité [52]
- Signatures courtes [20]
- Le schéma El Gamal de Verheul [75]
- Diffusion [36]

Beaucoup d'autres applications des couplages peuvent être consultées dans [27], [10, Chapter X].

Motivation et Objectifs de la Thèse

Considérant les applications sans cesse croissante des couplages en cryptographie, il est tout à fait important de s'interesser au calcul éfficace de ces applications. le calcul efficace du couplage dépend de l'arithmétique du modèle de la courbe elliptique choisi et du corps sur lequel cette courbe est définie. Dans la littérature, il existe plusieurs modèles parmi lesquels le modèle de Weierstrass d'equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, les modèles de Jacobi $E_a : \begin{cases} x^2 + y^2 = 1 \\ ax^2 + z^2 = 1 \end{cases}$, $E_{d,\alpha} : y^2 = dx^4 + 2\alpha x^2 + 1$, le modèle d'Edwards $x^2 + y^2 = c^2(1+x^2y^2)$, le modèle de Huff d'equation $ax(y^2-1) = by(x^2-1)$, le modèle Hessien d'equation $y^3 + x^3 + 1 = 3Dxy$. Les précédents travaux sur le calcul du couplage ont été fait sur le modèle d'Edwards d'une courbe elliptique successivement dans [21], [45] et [1]. Les récent résultats de calcul de couplage sur le modèle de Weierstrass se trouvent dans [18] ,[19] et dans [76] pour les quartiques de Jacobi. Le calcul du couplage de Tate sur le modèle Hessien de courbe elliptique se trouve dans [37] et dans [80] pour le modèle de Selmer. L'objectif de cette thèse est de calculer, améliorer et implémenter le couplage de Tate, Ate et ses variantes sur les modèles de courbes non encore étudiés à cet effet et de faire une étude comparative avec des résultats existants. Entre autre, de proposer de nouveaux modèles de courbes elliptiques et étudier leurs propriétés pour la cryptographie.

Contribution et Organisation de la Thèse

Ce manuscrit s'organise en quatre chapitres : le chapitre un donne des rappels mathématiques et les trois autres décrivent nos contributions.

Chapitre 1 : Rappels sur les courbes elliptiques et les couplages

Le **Chapitre** 1 présente les résultats fondamentaux sur les courbes elliptiques et les couplages, nécessaires à la compréhension du mémoire. Particulièrement nous définissons les courbes

elliptiques dans le contexte général du modèle de Weierstrass. Nous définissons aussi le concept des diviseurs sur une courbe elliptique et expliquons l'isomorphisme entre l'ensemble des points rationnels $E(\mathbb{K})$ d' une courbe elliptique E défini sur un corps $\mathbb{K}$ et sa Jacobienne. La methode de la tangente et sécante est présentée pour décrire la structure de groupe sur $E(\mathbb{K})$. Dans ce chapitre, nous étudions aussi la notion d'isomorphisme entre courbes elliptiques. Ceci permet de définir le concept de la tordue d'une courbe elliptique, très utile pour le calcul efficace du couplage. Les couplages de Weil et de Tate, ainsi que l'algorithme de Miller pour leurs calculs sont expliqués et quelques méthodes pour optimiser leurs calculs sont décrites. Nous rappellons, pour terminer le chapitre, les valeurs des paramètres à considérer pour la construction des protocoles cryptographiques sécurisés basés sur les coulages.

Chapitre 2 : Couplage de Tate sur les courbes de Jacobi

Le **Chapitre** 2 est notre première contribution et constitue un article avec Sylvain Dusquesne [26]. Il est concentré essentiellement sur le calcul du couplage de Tate par l'algorithme de Miller sur deux modèles de Jacobi de courbes elliptiques. L'exécution de cet algorithme nécessite une fonction spéciale appelée fonction de Miller qui est déduite de l'interprétation géométrique de la loi de groupe. Dans la première partie de ce chapitre, après avoir présenté les formules d'addition et l'interprétation géométrique de la loi de groupe, nous utilisons cette dernière pour déterminer la fonction de Miller sur les intersections des quadriques de Jacobi. Ce qui nous permet de calculer pour la prémière fois le couplage de Tate sur cette courbe. Nous définissons et utilisons la tordue quadratique pour optimiser les calculs. Les résultats obtenus sont efficaces et compétitives par rapport aux résultats sur les modèles de Weierstrass ou d'Edwards (voir Table 2.1). Dans la deuxième partie de ce chapitre, nous nous interessons à la quartique de Jacobi donnée par l'equation $Y^2 = dX^4 + Z^4$. Nous proposons un nouveau système des représentation des points pour obtenir de nouvelles formules d'addition. Nous définissons aussi la tordue d'ordre quatre de cette courbe. nous utilisons un isomorphisme entre le modèle de Weierstrass et cette quartique pour obtenir la fonction de Miller associée. Une implémentation avec le logiciel de calcul formel Magma et un exemple de courbe elliptique bien adaptée au calcul de couplage nous permet de vérifier nos résultats, qui constituent dès lors une amélioration de ceux obtenus récement sur la même courbe [76] et sont meilleurs, de l'ordre de 26%, que ceux obtenus sur le modèle de Weierstrass (voir tables 2.4 et 2.5).

Chapitre 3 : Couplages Ate et Optimal Ate sur les courbes de Jacobi

Le **Chapitre** 3 est un article soumis avec Nadia El Mrabet et Sylvain Duquesne [25]. Dans ce chapitre, nous nous intéressons au calcul des versions optimisées du couplage Ate sur la quartique spéciale de Jacobi $Y^2 = dX^4 + Z^4$ à savoir : le couplage Ate, le couplage Ate tordu et le couplage Ate optimal. En effet, dépuis le développement de la cryptographie basée sur les couplages, l'efficacité de l'algorithme de Miller, élément essentiel pour un calcul pratique du couplage, a été beaucoup amélioré. Une des voies d'amélioration étant la réduction du nombre d'itérations de cet algorithme, qui a conduit à de nouveaux couplages tels que le couplage Ate, le couplage optimal pouvant ête calculé en un nombre minimal d'itérations. Après avoir décrit ces différents couplages, nous reécrivons les formules d'addition et la fonction de Miller pour le calcul de ces couplages sur la quartique de Jacobi $Y^2 = dX^4 + Z^4$. Les résultats obtenus sont meilleurs, de l'ordre de 11%, que ceux sur le modèle de Weierstrass et sont dés lors les meilleurs résultats à nos jours, à notre connaissance, sur les courbes possédant des tordus d'ordre 4 (voir Table 3.3). Nous terminons le chapitre par une implémation avec le logiciel Magma, de ces différents couplages, ce qui nous permet en même temps de vérifier nos formules.

Chapitre 4 : Nouveau modèle d'Edwards en caractéristique quelconque

Le **Chapitre** 4 présente un travail commun avec Oumar Diao dont une partie est publiée dans [24]. Nous utilisons la théorie des fonctions thêta pour obtenir un nouveau modèle d'Edwards de courbes elliptiques, avec la particularité d'être défini en toutes caractéristiques. Un modèle intermédiaire, que nous appellons dans cette thèse modèle thêta de niveau 4, est utilisé. Pour cela, nous présentons dans les prémières sections de ce chapitre un rappel sur les corps $p-$adic , les fonctions thêta et les relations thêta de Riemann, pierres angulaires des résultats obtenus dans la suite. Nous commençons par définir le modèle thêta de niveau 4 ainsi que les formules d'addition sur cette courbe (voir Définition 34 et Théorème 22). Une $2-$ isogénie à ce modèle permet d'obtenir un nouveau modèle, défini en toute caractéristique et qui étend bien à la caractéristique 2 le modèle original d'Edwards [28] (voir Théorème 27). Nous étudions l'arithmétique de ces deux courbes (théorèmes 22 et 33). Nous démontrons que les lois de groupe, obtenues par les relations thêta de Riemann sont complètes et unifiées (voir Théorème 25). Bien que l'addition en caractéristiqique impaire ne soient pas compétitive, elle l'est en caractéristique 2 (Table 4.6). En particulier l'addition différentielle sur la ligne de Kummer du modèle thêta de niveau 4 est efficace, nécessite $4m_1 + 3s_1 + 2mc$, ce qui représente à nos jours la meilleure complexité en addition différentielle (Table 4.8).

Perspectives de recherche

Quelques idées à l'issue de cette thèse nous inspirent pour la recherche future :

- L'amélioration de l'arithmétique et l'utilisation de l'algorithme de Miller pour le calcul des couplages peuvent être developpés sur le modèle thêta de niveau 4 et sur le modèle d'Edwards proposé.
- Lubicz et Robert ont utilisés très récement les fonctions thêta pour améliorer le calcul des couplages en caractéristique impaire. Cette étude dévrait être faite en caractéristique 2 grâce à nos résultats.

Publications issues de la thèse

A l'issue de cette thèse, deux articles sont publiés et un autre soumis dans un journal.

1. *Tate pairing computation on Jacobi's elliptic curves* , avec Sylvain Duquesne : Pairing-Based Cryptography, Pairing 2012 : LNCS, Vol.7708, Springer. pp. 254-269 (2012).
2. *Efficient pairings computation on Jacobi quartic elliptic curve*, with Sylvain Duquesne and Nadia El Mrabet (soumis), available on the International Association of Cryptology Research web's page :`eprint.iacr.org/2013/597.pdf`
3. *Arithmetic of the Level Four theta model of ellitic curves*, avec Oumar Diao (Accepté pour publication à Afrika Mathematica, (DOI) 10.1007/s13370-013-0203-1 (Springer))

Chapitre UN

Review on elliptic curves and pairings

In this chapter, $\mathbb{K}$ denote a field and the algebraic closure is denoted $\overline{\mathbb{K}}$. The affine space of dimension n over $\mathbb{K}$ is the set of n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\overline{\mathbb{K}}) = \{(x_1, x_2, ..., x_n); x_i \in \overline{\mathbb{K}}, i = 1, ..., n\}$$

The projective space of dimension n denoted $\mathbb{P}^n$ is

$$\mathbb{P}^n(\overline{\mathbb{K}}) = \mathbb{A}^{n+1}(\overline{\mathbb{K}}) / \sim$$

where $\sim$ is the equivalence relation defined on $\mathbb{A}^{n+1}(\overline{\mathbb{K}}) \setminus (0, 0, ..., 0)$ by

$$(X_0, ..., X_n) \sim (Y_0, ..., Y_n)$$

if there exists $\lambda \in \overline{\mathbb{K}}^*$ with $X_i = \lambda Y_i$ for all $i = 0, 1, ..., n$. An equivalence class $\{(\lambda X_0, ..., \lambda X_n)\}$ is denoted $[X_0 : .... : X_n]$ and $X_0, ..., X_n$ are called homogeneous coordinates for the corresponding points in $\mathbb{P}^n$. The set of $\mathbb{K}$-rational points in $\mathbb{P}^n$ is the set $\mathbb{P}^n(\mathbb{K}) = \{[X_0 : .... : X_n]; X_i \in \mathbb{K}\}$. The set of projective points $\{[X_0 : .... : X_n]; X_i \in \mathbb{K}, i = 0, ..., n-1; X_n = 0\}$ is called the *line at infinity*.
The definitions and results stated in this chapter can be found in the books [77],[70],[10],[44],[2] and [38].

1.1 Background on elliptic curves

1.1.1 General definitions

Definition 1. *An elliptic curve over a field $\mathbb{K}$ is a pair (E, P_∞) where E is a smooth curve of genus one in the projective space and P_∞ is a rational point. In the projective space $\mathbb{P}^2(\overline{\mathbb{K}}) = \{[X : Y : Z]; X, Y, Z \in \mathbb{K}\}$, an elliptic curve is usually given by the following equation*

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \text{ with } a_i \in \mathbb{K}, i = 1, 2, 3, 4, 6. \quad (1.1)$$

The smoothness of the curve means that there is no points on the curve that satisfies the partial derivative equations :

$$\begin{aligned} a_1YZ - 3X^2 - 2a_2XZ - a_4Z^2 &= 0 \\ 2YZ + a_1XZ + a_3Z^2 &= 0 \\ Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2 &= 0 \end{aligned}$$

There is only one point which lies on the line at infinity and on the curve E. This point is $[0:1:0]$ and is called the *point at infinity*. The equation 1.1 is called the Weierstrass equation of an elliptic curve. Every elliptic curve can be written in Weierstrass form, and conversely, every smooth Weierstrass plane cubic curve is an elliptic curve [70].

Definition 2. *Let $\mathbb{L}$ be an extension field of $\mathbb{K}$. Then the set of $\mathbb{L}$-rational points on the curve E, denoted $E(\mathbb{L})$, is defined to be the set of points of the curve E with coordinates in $\mathbb{L}$.*

The affine version of the definition of an elliptic curve is given in the following definition.

Definition 3. *An elliptic curve E over a field $\mathbb{K}$ is the set of solution in $\mathbb{A}^2(\overline{\mathbb{K}})$ of the equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ with } (a_1, a_2, a_3, a_4, a_6) \in \mathbb{K}^5$$

together with the point at infinity $[0:1:0]$ and the condition $\Delta_E \neq 0$ where $\Delta_E = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$ with $d_2 = a_1^2 + 4a_2, d_4 = 2a_4 + a_1, d_6 = a_3^2 + 4a_6, d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$ The quantity Δ_E is called the discriminant of E and the condition $\Delta_E \neq 0$ ensures that the curve E is smooth.

From now on, $E(\mathbb{K})$ denoted the set of $\mathbb{K}$-rational points of E together with the point at infinity that we denote P_0.

1.1.2 Function field, divisors and Picard group of an elliptic curve

Function field of an elliptic curve

Definition 4. *Let E be an elliptic curve defined over $\mathbb{K}$ and let $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be its affine equation. Let $F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \in \mathbb{K}[x,y]$.*

1. *The coordinate ring $\mathbb{K}[E]$ of E over $\mathbb{K}$ is the integral domain $\mathbb{K}[E] = \mathbb{K}[x,y]/(F(x,y))$ since $F(x,y)$ is absolutely irreducible in $\mathbb{K}[x,y]$. Similarly we define $\overline{\mathbb{K}}[E] = \overline{\mathbb{K}}[x,y]/(F(x,y))$, the coordinate ring of E over $\overline{\mathbb{K}}$. The elements of $\overline{\mathbb{K}}[E]$ are called* regular functions.
2. *The function field $\mathbb{K}(E)$ of E over $\mathbb{K}$ is the fraction field of $\mathbb{K}[E]$. Similarly we define $\overline{\mathbb{K}}(E)$, the function field of E over $\overline{\mathbb{K}}$. The elements of $\overline{\mathbb{K}}(E)$ are called* rational functions.

Divisors on elliptic curves

Definition 5. *Let E be an elliptic curve defined over $\mathbb{K}$. For each point $P \in E(\overline{\mathbb{K}})$, define a formal symbol (P). A divisor is a formal sum of such symbols : $D = \sum_{P \in E(\overline{\mathbb{K}})} a_P(P)$ where $a_P \in \mathbb{Z}$ and all but finitely many a_P are zero.*

Definition 6. *Consider the following divisor $D = \sum_{P \in E(\overline{\mathbb{K}})} a_P(P)$.*

1. *The* degree *of D is the sum of its coefficients,* $\deg(D) = \sum_{P \in E(\overline{\mathbb{K}})} a_P$.
2. *The* support *of D is the set* $\mathrm{supp}(D) = \{P \in E(\overline{\mathbb{K}}) : a_P \neq 0\}$.
3. *Let σ be a Galois automorphism of $\mathbb{K}$. By definition $D^\sigma = \sum_{P \in E(\overline{\mathbb{K}})} a_P(\sigma(P))$.*
4. *The divisor D is defined over $\mathbb{K}$ if $D^\sigma = D$ for all Galois automorphism σ of $\mathbb{K}$.*

The set $\mathrm{Div}(E)$ of divisors on $E(\overline{\mathbb{K}})$ forms a free abelian group where the addition $+$ is defined as follows : Let $D = \sum_{P \in E(\overline{\mathbb{K}})} a_P(P)$ and $D = \sum_{P \in E(\overline{\mathbb{K}})} b_P(P)$ be two divisors then

$$D + D' = \sum_{P \in E(\overline{\mathbb{K}})} (a_P + b_P)(P)$$

Divisors of functions

Let $f \in \overline{\mathbb{K}}(E)$ and $P \in E(\overline{\mathbb{K}})$. The function f is said to have a **zero** at P if it takes the value 0 at P , and it has a **pole** at P if it takes the value ∞ at P. In order to define the order of the pole or the zero of f, it can be shown [70, Page 22] that there is a function u_P, called a **uniformizer** at P, with $u(P) = 0$ and such that the function f can be written in the form

$$f = u_P^r g, \text{ with } r \in \mathbb{Z} \text{ and } g(P) \neq 0, \infty.$$

Define the order of f at P by $\mathrm{ord}_P(f) = r$. On can show that for any function $f \in \overline{\mathbb{K}}(E)$, there is only finitely many points of E where f has a pole or a zero. Further, if f has no zero or pole then f is a non zero constant [39, Section 2]. These comments make sense to the following definition.

Definition 7. ***(Divisor of function)*** *Let f be a rational function on E, then the divisor of f is* $\mathrm{Div}(f) = \sum_{P \in E(\overline{\mathbb{K}})} ord_P(f)(P)$ *where $ord_P(f)$ is the order of the zero or the pole of f at P. If f has no zero or pole at P, then* $\mathrm{Div}(f) = 0$, *the null divisor.*

An important property of divisors of functions is stated in the following proposition :

Proposition 1. *[10, Section IX.2] Let f and g be two rationals functions. Then*

1. $\mathrm{Div}(f \times g) = \mathrm{Div}(f) + \mathrm{Div}(g)$
2. $\mathrm{Div}(\frac{f}{g}) = \mathrm{Div}(f) - \mathrm{Div}(g)$

Definition 8. *A divisor D is called a principal divisor if there exists a function $f \in \overline{\mathbb{K}}(E)$ such that $D = \mathrm{Div}(f)$. Two divisors D_1 and D_2 are said linearly equivalent, denoted $D_1 \sim D_2$, if $D_1 - D_2$ is a principal divisor. The* ***divisor class group****(or* ***Picard group****) of E, denoted* $\mathrm{Pic}(E)$ *is the quotient of* $\mathrm{Div}(E)$ *of divisors on E by the subgroup* $\mathrm{Princ}(E)$ *of principal divisors on E.*

The degree of the divisor of a function is always 0 [39, Section 2]. It follows that $\mathrm{Princ}(E)$ is a subgroup of $\mathrm{Div}^0(E)$, the set of zero's degree divisors. The subset $\mathrm{Pic}^0(E)$ is the quotient of $\mathrm{Div}^0(E)$ by the subgroup $\mathrm{Princ}(E)$. We denote $\mathrm{Pic}^0_{\mathbb{K}}(E)$ the subgroup of $\mathrm{Pic}^0(E)$ invariant under the action of any Galois automorphism of $\mathbb{K}$. The following proposition enables to define a group structure in $E(\mathbb{K})$.

Proposition 2. *[70, Page 66] Let E be an elliptic curve defined over $\mathbb{K}$.*

1. *For two arbitrary points P and Q of E, $(P) \sim (Q)$ iff $P = Q$.*
2. *For any divisor $D \in \mathrm{Div}^0_{\mathbb{K}}(E)$, there exists a unique point P of E such that $D \sim (P) - (P_0)$. Let $\sigma : \mathrm{Div}^0_{\mathbb{K}}(E) \to E(\mathbb{K})$ the map given by this association.*
3. *σ is surjective.*
4. *Let $D_1, D_2 \in \mathrm{Div}^0_{\mathbb{K}}(E)$. Then $\sigma(D_1) = \sigma(D_2)$ iff $D_1 \sim D_2$. Thus σ induces a bijection :*

$$\mathrm{Pic}^0_{\mathbb{K}}(E) \simeq E(\mathbb{K})$$

It follows immediately from this proposition that one can define a group law on the set $E(\mathbb{K})$ of rational points of E, which is exactly the group law induced from $\mathrm{Pic}^0_{\mathbb{K}}(E)$ by using σ.

Group law

The group law in $E(\mathbb{K})$ has the following geometric interpretation in the set of real numbers $\mathbb{R}$: Given the points P and Q, draw the line through P and Q (draw the tangent to the elliptic curve at P if $P = Q$). This line intersects the elliptic curve at a third point. Then the sum R of P and Q is the reflection of this point about the x-axis. This is depicted in figure 4.1.

Explicit formulas are given in the following theorem :

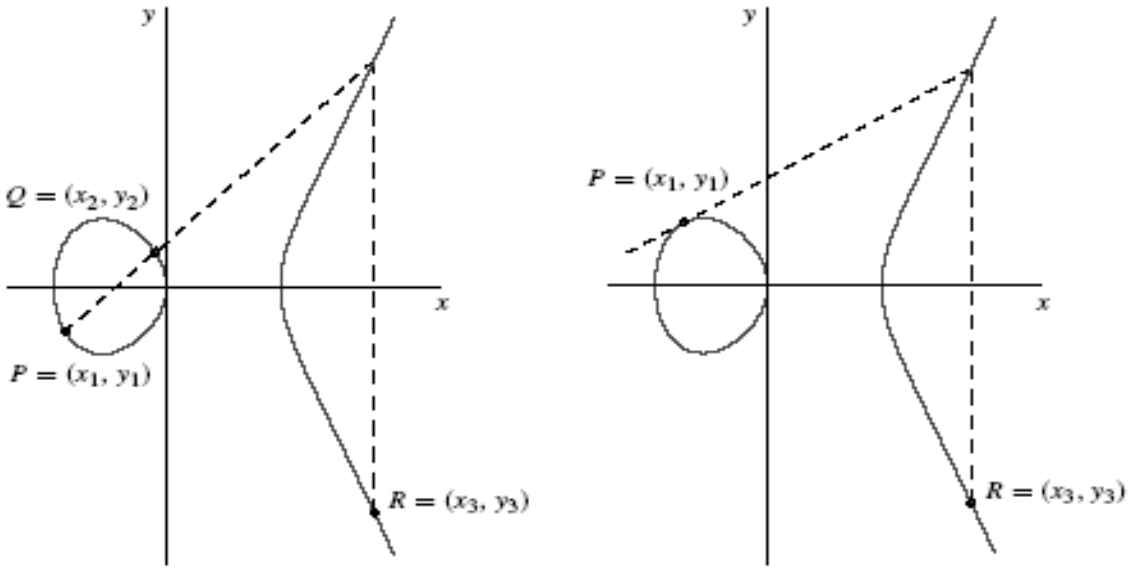

FIGURE 1.1 – Addition and doubling of elliptic curve points in the set of real numbers $\mathbb{R}$.

Theorem 1. *The set $E(\mathbb{K})$ is an abelian group under the addition $+$ defined as follows :*

- *Let $P = (x_1, y_1) \in E(\mathbb{K})$. Then*

$$P + P_0 = P_0 + P = P and - P = (x_1, -y_1 - a_1x_1 - a_3)$$

- *Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two elements of $E(\mathbb{K})$. The coordinates of $R = (x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ are defined as follows :*
  - *If $P = -Q$ then $P + Q = P_0$ else*
  - *The coordinates (x_3, y_3) of the point $R = P + Q$ are :*

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 = -(\lambda + a_1)x_3 - \nu - a_3, \end{cases}$$

with

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P_1 \neq P_2, \\ (3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)/(2y_1 + a_1x_1 + a_3) & \text{if } P_1 = P_2. \end{cases}$$

and

$$\nu = y_1 - \lambda x_1$$

As a consequence of proposition 2, we have in the following theorem, a characterisation of divisors of functions.

Theorem 2. *[70, Corollary 3.5, Page 67] A divisor D is a principal divisor if and only if*

$$deg(D) = 0 \text{ and } \sum_{P \in E(\overline{\mathbb{K}})} a_P P = P_\infty$$

The following theorem will be useful in section 1.3.

Theorem 3. *Weil Reciprocity [77, Lemma 11.11] Consider the divisor* $D = \sum_{P \in E(\overline{\mathbb{K}})} a_P(P)$. *The image by* f *of* D *is defined as* $f(D) = \prod_{P \in E(\overline{\mathbb{K}})} f(P)^{a_P}$.
Suppose that D *is a principal divisor. Then there exists a function* g *such that* $D = \mathrm{Div}(g)$. *If the supports of* $\mathrm{Div}(g)$ *and* $\mathrm{Div}(f)$ *are disjoint, then we have* $f(\mathrm{Div}(g)) = g(\mathrm{Div}(f))$. *This equality is called* ***Weil reciprocity*** .

1.1.3 Elliptic curves over finite fields

We consider the finite field $\mathbb{K} = \mathbb{F}_q$. Since the Weierstrass equation has at most two solutions for each $x \in \mathbb{F}_q$, we conclude that $\sharp E(\mathbb{F}_q)$ is finite and $\sharp E(\mathbb{F}_q) \in [1, 2q+1]$. In cryptography, it is important to know the order of this group. Hasse's theorem provides tighter bounds for $\sharp E(\mathbb{F}_q)$.

Theorem 4. *(Hasse)[77, Theorem 4.2] Let* E *be an elliptic curve defined over a finite field* $\mathbb{F}_q$. *Then*

$$q + 1 - 2\sqrt{q} \leq \sharp E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

The structure of this group is given in the following theorem.

Theorem 5. *[38, Theorem 3.12] Let* E *be an elliptic curve defined over a finite field* $\mathbb{F}_q$, *then there exists two integers* d_1 *and* d_2 *such that*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}, \quad d_1 | d_2$$

The following two propositions enable in some cases to determine $\sharp E(\mathbb{F}_q)$.

Theorem 6. *[77, Theorem 4.12] Let* E *be an elliptic curve defined over a finite field* $\mathbb{F}_q$. *Suppose that one knows that* $\sharp E(\mathbb{F}_q) = q + 1 - a$. *Then*

$$\forall n \geq 1,\ \sharp E(\mathbb{F}_{q^n}) = q^n + 1 - S_n$$

where (S_n) *is the sequence defined as follows :* $S_0 = 2$, $S_1 = a$ *et* $S_{n+1} = aS_n - qS_{n-1}$.

Theorem 7. *[77, Theorem 4.14] Let* E *be an elliptic curve defined over a finite field* $\mathbb{F}_q$. *Then*

$$\sharp E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right)$$

where

$$\left(\frac{x}{\mathbb{F}_q} \right) = \begin{cases} 1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^* \\ -1 & \text{if } t^2 = x \text{ doesn't have a solution } t \in \mathbb{F}_q^* \\ 0 & \text{if } x = 0 \end{cases}$$

is the generalised Legendre symbol.

1.1.4 Torsion points

The points of finite order play an important role in elliptic curve cryptography. We give the definition and the structure of the group of torsion points.

Definition 9. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, n is a non zero integer. The set*

$$E(\overline{\mathbb{F}_q})[n] = \{P \in E(\overline{\mathbb{F}_q}) : nP = P_0\}$$

is the set of $n-$torsion points. That is the set of points of order n with coordinates in $\overline{\mathbb{F}_q}$.

$E(\overline{\mathbb{F}_q})[n]$ is a subgroup of $E(\overline{\mathbb{F}_q})$ since it is the kernel of the morphism $P \mapsto nP$, see section 1.2 for morphisms of elliptic curves. Sometimes we will write $E[n]$ instead of $E(\overline{\mathbb{F}_q})[n]$ to simplify notations. The structure of this group is given in the following theorem.

Theorem 8. *[77, Theorem 3.2] Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ and n be a non zero integer.*

1. *If the characteristic p is 0 or does not divide n, then*
$$E[n] \backsimeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$
2. *If the characteristic p divides n , then we can write $n = p^r n'$ with $p \nmid n'$ for a certain n'. Then*
$$E[n] \backsimeq \mathbb{Z}/n'\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \text{ or } E[n] \backsimeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z}$$

Definition 10. *An elliptic curve E defined over a field of characteristic p, is called **ordinary** if $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$. It is called **supersingular** if $E[p] \simeq \{P_0\}$.*

Definition 11. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Let r be a prime integer dividing $\sharp E(\mathbb{F}_q)$. The embedding degree of E with respect to r is the smallest integer k such that r divides $q^k - 1$.*

The following theorem shows that the embedding degree specifies the minimal extension field which contains all the torsion points.

Theorem 9. *(Balasubramanian and Koblitz [3]) Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Let r be a prime integer dividing $\sharp E(\mathbb{F}_q)$. Suppose that r does not divide $q-1$ and that $gcd(r, q) = 1$. Then $E(\overline{\mathbb{F}_q})[r] \subset E(\mathbb{F}_{q^k})$ if and only if r divides $q^k - 1$.*

1.2 Morphisms and twists of elliptic curves

In this section we recall morphisms of elliptic curves and especially the notion of twists of elliptic curves. The book of Silvermann is a good reference [70].

1.2.1 Morphisms of elliptic curves

Let E_1 and E_2 be two affine elliptic curves defined over a field $\mathbb{K}$.

1. A rational map from E_1 to E_2 is a map of the form $\phi : E_1 \to E_2$, $\phi = [g, h]$ where $g, h \in \mathbb{K}(E_1)$, the function field of E_1, have the property that for every point $P \in E_1$ at which g and h are defined $\phi(P) = (g(P), h(P)) \in E_2$.
   A rational map that is defined at every point is called a morphism.
2. A ratinal map $\phi : E_1 \to E_2$ defined over $\mathbb{K}$ is a birational equivalence over $\mathbb{K}$ if there exits a rational map $\varphi : E_2 \to E_1$ such that $\varphi \circ \phi(P) = P$ for all point $P \in E_1(\overline{\mathbb{K}})$ such that $\varphi \circ \phi(P)$ is defined and $\phi \circ \varphi(P) = P$ for all point $P \in E_2(\overline{\mathbb{K}})$ such that $\phi \circ \varphi(P)$ is defined.
3. An isogeny is a morphism $\phi : E_1 \to E_2$ satisfying $\phi(P_0) = P_0$
4. An endomorphism on E_1 is an isogeny $\phi : E_1 \to E_1$
5. An isogeny $\phi : E_1 \to E_2$ is an isomorphism if there exists an isogeny $\psi : E_2 \to E_1$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are identity maps on E_2 and E_1 respectively.
6. An endomorphism on E_1 is called an automorphism of E_1 if it is also an isomorphism.

The Frobenius endomorphism

Let us consider an endomorphism

$$\begin{array}{rccl} \alpha : & E(\overline{\mathbb{K}}) & \to & E(\overline{\mathbb{K}}) \\ & (x, y) & \mapsto & \alpha(x, y) = (g(x, y), h(x, y)) \end{array}$$

According to [77, Chapter 3-4] we can write $g(x, y)$ in the form $\frac{p(x)}{q(x)}$ using the equation of the elliptic curve E. The minimum of the degrees of the polynomials $p(x)$ and $q(x)$ is called the *degree* of the endomorphism α, denoted $\deg(\alpha)$. Let n be an integer such that the characteristic of $\mathbb{K}$ does not divides n or is 0. Then according to theorem 8, $E[n]$ is a 2-dimensional vector space over $\mathbb{Z}/n\mathbb{Z}$. Denote $\{P_1, P_2\}$ a basis of $E[n]$, and because α maps $E[n]$ to $E[n]$, there are a, b, c and d in $\mathbb{Z}/n\mathbb{Z}$ such that

$$\alpha(P_1) = aP_1 + cP_2 \text{ and } \alpha(P_2) = bP_1 + dP_2$$

Therefore, each endomorphism is represented by a 2×2 matrix

$$\alpha_n = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

describing its action on the basis $\{P_1, P_2\}$ of $E[n]$. The trace of the matrix α_n is called the trace of the endomorphism α and is denoted $\mathrm{tr}(\alpha)$. The following proposition comes from [77, Chapter 3-4].

Proposition 3. *Let $\alpha : E(\overline{\mathbb{K}}) \to E(\overline{\mathbb{K}})$ be an endomorphism of elliptic curve. Let n be an integer such that the characteristic of $\mathbb{K}$ does not divides n or is 0 and α_n the matrix that describes the action of α on a basis of $E[n]$. Then*

$$\deg(\alpha) = \sharp\mathrm{Ker}(\alpha) = \det(\alpha_n)$$

where $\det(\alpha_n)$ is the determinant of the matrix α_n.

We are now in position to define the Frobenius endomorphism and give some properties. Consider the following map :

$$\begin{array}{rccl} \pi_q : & E(\overline{\mathbb{F}_q}) & \to & E(\overline{\mathbb{F}_q}) \\ & (x,y) & \mapsto & \pi_q(x,y) = (x^q, y^q) \\ & P_0 & \mapsto & \pi_q(P_0) = P_0 \end{array}$$

We can easily prove the following proposition :

Proposition 4. *The map π_q satisfies the following properties :*

1. *π_q is an endomorphism of elliptic curve, called the **Frobenius endomorphism**.*
2. *$\pi_q(E(\mathbb{F}_q)) = E(\mathbb{F}_q)$*
3. *$\deg(\pi_q) = q$*

In what follows, we study isomorphisms between elliptic curves.

Proposition 5. *Two elliptic curves E_a and E_b defined over a field $\mathbb{K}$ by :*

$$E_a : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$E_b : y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$$

are isomorphic over $\mathbb{K}$ iff

$$\exists (u,r,s,t) \in \mathbb{K}^\star \times \mathbb{K}^3, s.t \begin{cases} ub_1 &= a_1 + 2s, \\ u^2b_2 &= a_2 - sa_1 + 3r - s^2, \\ u^3b_3 &= a_3 + ra_1 + 2t, \\ u^4b_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\ u^6b_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{cases}$$

The isomorphism between E_a and E_b is defined as follows :

$$\begin{array}{rccl} \sigma : & E_a & \to & E_b \\ & (x,y) & \mapsto & (u^2x + r, u^3y + u^2sx + t) \end{array}$$

If $(u,r,s,t) \in \overline{\mathbb{K}}^\star \times \overline{\mathbb{K}}^3$ then we said that the curves are isomorphic over $\overline{\mathbb{K}}$.

Example Consider the elliptic curve $E_a : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ defined over the field $\mathbb{K}$. If the characteristic of $\mathbb{K}$ is not 2 then

$$\begin{array}{rccc} \sigma : & E & \to & E' \\ & (x,y) & \mapsto & (x, y + \frac{1}{2}(a_1x + a_3)) \end{array}$$

is an isomorphism from E to the elliptic curve $E' : y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$ where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^3 + 4a_6$.
If in addition the characteristic is different from 3, then

$$\begin{array}{rccc} \sigma : & E' & \to & E'' \\ & (x,y) & \mapsto & (x + \frac{b_2}{12}, y) \end{array}$$

is an isomorphism from E' to the elliptic curve $E'' : y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$ where $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.
The notion of isomorphism of elliptic curve is closed to the concept of j-invariant as shown in theorem 10.

Definition 12. *The j-invariant of an elliptic curve $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ defined over $\mathbb{K}$ is the quantity*

$$j_E = \frac{c_4^3}{\Delta_E}$$

where $c_4 = d_2^2 - 24d_4$ and Δ_E is the discriminant of the curve following the notation in definition 3.

We then have the following result

Theorem 10. *[77, Theorem 2.19] If two elliptic curves E and E' defined over a field $\mathbb{K}$ are isomorphic over $\mathbb{K}$, then they have the same j-invariant. The converse is true if $\mathbb{K}$ is algebraically closed.*

In the following proposition, we give the simplest form of elliptic curve up to isomorphism in each characteristic.

Proposition 6. *[2, Section 4.2.2] Let $E' : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve defined over $\mathbb{K}$. Then there exists an isomorphism $(x,y) \mapsto (u^2x + r, u^3y + u^2sx + t)$ from E' to a simplest form elliptic curve E defined over $\mathbb{K}$ in the following table.*

Char($\mathbb{K}$)	*Equation of E*	Δ	*j-invariant*
$\neq 2, \neq 3$	$y^2 = x^3 + a_4x + a_6$	$-16(4a_4^3 + 27a_6^2)$	$1728a_4^3/4\Delta$
3	$y^2 = x^3 + a_4x + a_6$	$-a_4^3$	0
3	$y^2 = x^3 + a_2x^2 + a_6$	$-a_2^3a_6$	$-a_2^3/a_6$
2	$y^2 + a_3y = x^3 + a_4x + a_6$	a_3^4	0
2	$y^2 + xy = x^3 + a_2x^2 + a_6$	a_6	$1/a_6$

1.2.2 Twists of elliptic curves

Definition 13. *A twist of an elliptic curve E defined over a field $\mathbb{K}$ is an elliptic curve E' defined over $\mathbb{K}$ which is isomorphic to E over an algebraic closure $\mathbb{K}'$ of $\mathbb{K}$. The degree of the twist is the minimal degree of the extension $\mathbb{K}'$ over $\mathbb{K}$ such that E is isomorphic to E' over $\mathbb{K}'$.*

In the following proposition we give the twists of elliptic curves given in short Weierstrass form, the corresponding isomorphism and the twist degree depending on the j-invariant of the curve. See also [70, Proposition 5.4] or [2, Corollary 13.16].

Proposition 7. *[19, Section 2] Let d' and k be two integers such that d' divides k. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over the finite field $\mathbb{F}_{q^{k/d'}}$ of characteristic different from 2 and 3. Let $\omega \in \mathbb{F}^{\star}_{q^k}$ and denote by E_ω the twist of E with respect to ω. Denote $\sigma_\omega : E_\omega \to E$ the isomorphism between the elliptic curve E and its twist E_ω, d' the degree of the twist. then we have*

j_E	*Field of definition for powers of* ω	d'	E_ω	σ_ω
$\notin \{0, 1728\}$	$\omega^2, \omega^4, \omega^6 \in \mathbb{F}_{q^{k/2}}, \omega^4 \in \mathbb{F}_{q^{k/4}}$ $\omega^3 \in \mathbb{F}_{q^k}$, $\omega^3 \notin \mathbb{F}_{q^{k/2}}$	2	$y^2 = x^3 + \omega^4 ax + \omega^6 b$	$(x, y) \mapsto (\omega^{-2}x, \omega^{-3}y)$
0	$\omega^3, \omega^6 \in \mathbb{F}_{q^{k/3}}$ $\omega^2 \in \mathbb{F}_{q^k}, \omega^2 \notin \mathbb{F}_{q^{k/3}}$	3	$y^2 = x^3 + \omega^6 b$	$(x, y) \mapsto (\omega^{-2}x, \omega^{-3}y)$
1728	$\omega^2 \in \mathbb{F}_{q^{k/2}}, \omega^4 \in \mathbb{F}_{q^{k/4}}$ $\omega^3 \in \mathbb{F}_{q^k}$ $\omega^3 \notin \mathbb{F}_{q^{k/2}}$	4	$y^2 = x^3 + \omega^4 ax$	$(x, y) \mapsto (\omega^{-2}x, \omega^{-3}y)$
0	$\omega^3 \in \mathbb{F}_{q^{k/3}}, \omega^6 \in \mathbb{F}_{q^{k/6}}$ $\omega^2 \in \mathbb{F}_{q^{k/2}}$	6	$y^2 = x^3 + \omega^6 b$	$(x, y) \mapsto (\omega^{-2}x, \omega^{-3}y)$

1.3 Bilinear pairings

In this section, we recall the Tate pairing on elliptic curves defined over finite fields. We then explain the Miller algorithm for its efficient computation. Most of the results stated in this section are taken from the following books : [77, Chapter 11], [2, Chapter 6], [10, Part 4] and [32].

1.3.1 The Tate pairing

The Tate pairing over finite fields is the most important pairing on elliptic curves introduced in cryptography by Frey and Rück in [31]. The first definition of the Tate pairing is due to Tate

on abelian varieties over local fields. Lichtenbaun [53] defined it in the case of Jacobian of curves to enable real computation. Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Let r be an integer co-prime to q dividing $\sharp E(\mathbb{F}_q)$. The embedding degree with respect to r is k. The set of $r-$th roots of unity in $\mathbb{F}_{q^k}$ is denoted μ_r. We also defined the sets $rE(\mathbb{F}_q) = \{rP, P \in E(\mathbb{F}_q)\}$ and $(\mathbb{F}_q^\star)^r = \{u^r, u \in \mathbb{F}_q^\star\}$. The quotient group $E(\mathbb{F}_q)/rE(\mathbb{F}_q)$ is the set of equivalence classes of points in $E(\mathbb{F}_q)$ under the equivalence relation $P_1 \equiv P_2$ if and only if $(P_1 - P_2) \in rE(\mathbb{F}_q)$. The quotient group $\mathbb{F}_q^\star/(\mathbb{F}_q^\star)^r$ is the set of equivalence classes of elements in $\mathbb{F}_q^\star$ under the equivalence relation $u \equiv v$ if and only if $\frac{u}{v} \in (\mathbb{F}_q^\star)^r$. To define the Tate pairing we take a point $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$. Since $rP = P_0$ there is a function $f_{r,P}$ with divisor $\mathrm{Div}(f_{r,P}) = r(P) - r(P_0)$ (Theorem 2). Let D_Q be any degree zero divisor defined over $\mathbb{F}_{q^k}$ and equivalent to $(Q) - (P_0)$ such that the support of D_Q is different from the support of $\mathrm{Div}(f_{r,P})$. One can note that $f_{r,P}(D_Q) \in \mathbb{F}_{q^k}^\star$ since D_Q and $\mathrm{Div}(f_{r,P})$ are defined over $\mathbb{F}_{q^k}^\star$ and have disjoint supports.

Definition 14. *The Tate pairing is the map*

$$\begin{array}{rccl} e_r: & E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) & \to & \mathbb{F}_{q^k}^\star/(\mathbb{F}_{q^k}^\star)^r \\ & (P, Q) & \mapsto & e_r(P,Q) = f_{r,P}(D_Q) \end{array}$$

To obtain a suitable form of the Tate pairing for a good computation, we make the following remarks.

Remark 1. *The Tate pairing is well defined as an element of $\mathbb{F}_{q^k}^\star/(\mathbb{F}_{q^k}^\star)^r$; i.e. if D_Q and D'_Q are two equivalent divisors then $\frac{f_{r,P}(D_Q)}{f_{r,P}(D'_Q)} \in (\mathbb{F}_{q^k}^\star)^r$.*

Remark 2. *The value of the Tate pairing is an equivalence class in $\mathbb{F}_{q^k}^\star/(\mathbb{F}_{q^k}^\star)^r$ and for cryptographic purposes one would like a unique representative of this class. This is obtained by raising $f_{r,P}(D_Q)$ to the power $(q^k - 1)/r$.*

Remark 3. *We assume that $k > 1$, that is $q - 1$ divides $(q^k - 1)/r$. We want to show that, in the definition of e_r, one can take $f_{r,P}(Q)$ instead of $f_{r,P}(D_Q)$. For an arbitrary point $R \in E(\mathbb{F}_q)$ different from $-P$ and P_0 consider the function $f'_{r,P}$ with divisor $\mathrm{Div}(f'_{r,P}) = r(P+R) - r(R)$. Then $f'_{r,P}(D_Q) \equiv f_{r,P}(D_Q)$. Indeed consider the function h corresponding to the addition of P and R, that is $\mathrm{Div}(h) = (P+R)-(R)-(P)+(P_0)$. Then $\mathrm{Div}(f'_{r,P}) = r(R+P)-r(R) = r\mathrm{Div}(h)+\mathrm{Div}(f_{r,P})$ implies $f'_{r,P} = f_{r,P}h^r$. Thus up to power $(q^k - 1)/r$ we have $(f'_{r,P}(D_Q))^{(q^k-1)/r} = (f_{r,P}(D_Q))^{(q^k-1)/r}$ since h is defined over $\mathbb{F}_q$. But $f'_{r,P}(D_Q) = f'_{r,P}((Q) - (P_0)) = \frac{f'_{r,P}(Q)}{f'_{r,P}(P_0)}$. Since P_0 is neither a pole nor a zero of $f'_{r,P}$ then $f'_{r,P}(P_0) \in \mathbb{F}_q^\star$ such that $(f'_{r,P}(P_0))^{(q^k-1)/r} = 1$. So $f'_{r,P}(D_Q) = (f'_{r,P}(Q))^{(q^k-1)/r}$. Since P and Q are fixed and R arbitrary can be taken variable, we conclude that $f'_{r,P}(Q)$ is constant when viewed as a function of R and thus coincides with $f_{r,P}(Q)$.*

Remark 4. *[10, Lemma IX.8] Since $\mathbb{F}_{q^k}$ is the smallest field containing both μ_r and $\mathbb{F}_q$ it follows that for every intermediate field L such that $\mathbb{F}_q \subseteq L \subset \mathbb{F}_{q^k}$, we have $L \subseteq (\mathbb{F}_{q^k}^\star)^r$. This means that the Tate pairing is trivial if P and Q belong to the same sub-field of $\mathbb{F}_{q^k}^\star$ containing $\mathbb{F}_q$, i.e $e_r(P,Q) \in (\mathbb{F}_{q^k}^\star)^r$.*

Remark 5. *One can show that if r^2 doesn't divide $\sharp E(\mathbb{F}_q)$ then $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ is isomorphic to the group $E(\mathbb{F}_{q^k})[r]$. It means that in this condition Q can be taken as a point of order r with coordinates in the extension field $\mathbb{F}_{q^k}$.*

These observations lead to the following definition of Tate pairing that we will use in this thesis.

Definition 15. *Reduced Tate Pairing*
Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Let r be an integer co-prime to q dividing $\sharp E(\mathbb{F}_q)$ such that r^2 doesn't divide $\sharp E(\mathbb{F}_q)$. The embedding degree with respect to r is $k > 1$. The set of $r-$th roots of unity in $\mathbb{F}_{q^k}$ is denoted μ_r. The reduced Tate pairing is the map :

$$\begin{array}{rccc} e_T : & E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] & \rightarrow & \mu_r \\ & (P,Q) & \mapsto & f_{r,P}(Q)^{\frac{q^k-1}{r}} \end{array}$$

Of course, according to the definition of pairings, the Tate pairing is bilinear and non degenerate.
Before we give an important property of the Tate pairing, observe that if $N = hr$ is a multiple of r which divides $q^k - 1$, then according to proposition 1 page 12 the function $f_{r,P}^h$ has divisor $\mathrm{Div}(f_{r,P}^h) = N(P) - N(P_0)$ and enables to prove the following result.

Proposition 8. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Let r be an integer co-prime to q dividing $\sharp E(\mathbb{F}_q)$ such that r^2 doesn't divide $\sharp E(\mathbb{F}_q)$. The embedding degree with respect to r is $k > 1$. Let $N = hr$ be a multiple of r which divides $q^k - 1$.*

1. *Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$. Then*

$$f_{N,P}(Q)^{\frac{q^k-1}{N}} = f_{r,P}(Q)^{\frac{q^k-1}{r}}$$

2. *Let $P \in E(\mathbb{F}_q)[N]$ and $Q \in E(\mathbb{F}_{q^k})[r]$. Then*

$$f_{N,P}(Q)^{\frac{q^k-1}{r}} = f_{r,hP}(Q)^{\frac{q^k-1}{r}}$$

1.3.2 The Weil pairing

We give in this section the definition of the Weil pairing which is closed to the definition of the Tate pairing. The notations are the same as in the case of Tate pairing but the points

P and Q are both elements of $E(\mathbb{F}_q)[r]$. It means that there exists two functions $f_{r,P}$ and $f_{r,Q}$ such that $\mathrm{Div}(f_{r,P}) = r(P) - r(P_0)$ and $\mathrm{Div}(f_{r,Q}) = r(Q) - r(P_0)$. Let D_P and D_Q be two degree zero divisors with disjoint supports, D_P equivalent to $(P) - (P_0)$ and D_Q equivalent to $(Q) - (P_0)$.

Definition 16. *The Weil pairing is the map*

$$\begin{array}{rccl} W_r: & E(\mathbb{F}_q)[r] \times E(\mathbb{F}_q)[r] & \to & \mathbb{F}^\star_{q^k}/(\mathbb{F}^\star_{q^k})^r \\ & (P,Q) & \mapsto & W_r(P,Q) = \frac{f_{r,P}(D_Q)}{f_{r,Q}(D_P)} \end{array}$$

Remark 6. *Observe that in the Weil pairing the numerator is equivalent modulo r-th power to $e_r(P,Q)$ while the denominator is equivalent modulo r-th power to $e_r(Q,P)$ such that we can write*

$$W_r(P,Q) = \frac{e_r(P,Q)}{e_r(Q,P)}$$

up to r-th power.

1.3.3 The Miller algorithm for pairings computation

In this section, we show how to determine $f_{r,P}(Q)$ using Miller's algorithm [58]. For an integer i, consider the divisor $D_i = i(P) - (iP) - (i-1)(P_0)$. We observe that D_i is a principal divisor, then according to theorem 2 page 13, there is a function f_i such that $\mathrm{Div}(f_{i,P}) = i(P) - (iP) - (i-1)(P_0)$. Observe that

$$\text{For } i = r \text{ one has } D_r = r(P) - r(P_0) = \mathrm{Div}(f_{r,P})$$

Thus, to obtain the value of $f_{r,P}(Q)$, it suffices to apply an iterative algorithm using an *addition chain* for r, that is, a sequence $(1, i_1, i_2, ..., r)$ such that each i_k is the sum of two previous terms of the sequence, see [2, Chapter 9] for more details on addition chain. Before we give the Miller algorithm, let us show that the functions $f_{i,P}$ can be chosen to satisfy the following conditions :

Lemma 7. *The functions $f_{i,P}$ satisfy the following conditions :*

1. $f_{1,P} = 1$
2. $f_{i+j,P} = f_{i,P} f_{j,P} \frac{\ell_{[i]P,[j]P}}{d_{[i+j]P}}$
3. $f_{ij,P} = f^j_{i,P} f_{j,[i]P} = f^i_{j,P} f_{i,[j]P}$

Where $\ell_{iP,jP}$ is the straight line defining $[i]P + [j]P$ and $d_{[i+j]P}$ the corresponding vertical line passing through $[i+j]P$.

Proof : The first assertion is clear because $\mathrm{Div}(f_{1,P}) = 0$, the null divisor. Then f_1 is constant.
For the second part we have : $\mathrm{Div}(\ell_{[i]P,[j]P}) = ([i]P)+([j]P)+(i+j)(P)-3(P_0)$ and $\mathrm{Div}(d_{[i+j]P}) = ([i+j]P) + (-[i+j]P) - 2(P_0)$. We apply proposition 1 page 12 to f_{i+j} and a straightforward calculation leads to $D_{i+j} = \mathrm{Div}(f_{i+j}) = (i+j)(P) - ([i+j]P) - (i+j-1)(P_0)$. We follow the same approach to prove the third property.
Now we can observe that

$$\mathrm{Div}\left(\frac{\ell_{[i]P,[j]P}}{d_{[i+j]P}}\right) = ([i]P) + ([j]P) - ([i]P + [j]P) - (P_0)$$

such that if $h_{R,S}$ is a rational function such that $\mathrm{Div}(h_{R,S}) = (R) + (S) - (S+R) - (P_0)$ where R and S are two arbitrary points of E, then the Miller algorithm in the general context of elliptic curve that computes efficiently the pairing of two points is stated as follows :

Algorithm 1 : Miller's Algorithm
Input : $P \in E(\mathbb{F}_q)[r]$, $Q \in E(\mathbb{F}_{q^k})[r]$, $r = (r_{n-1}, r_{n-2}, ...r_1, r_0)_2$, $r_{n-1} = 1$.
Output : The Tate pairing of P and Q : $f_{r,P}(Q)^{\frac{q^k-1}{r}}$

1 : Set $f \leftarrow 1$ and $R \leftarrow P$
2 : **For** $i = n-2$ **down to** 0 **do**
3 : $f \leftarrow f^2 \cdot h_{R,R}(Q)$
4 : $R \leftarrow 2R$
5 : **if** $r_i = 1$ **then**
6 : $f \leftarrow f \cdot h_{R,P}(Q)$
7 : $R \leftarrow R + P$
8 : **end if**
9 : **end for**
10 : **return** $f^{\frac{q^k-1}{r}}$

Some optimisations

We recall here some technicals that can be used for efficient implementation of the Miller algorithm. These technicals are summarised in [30].

1. **Use of twists of elliptic curves.** Many authors have shown that one can use twists of elliptic curves for an efficient computation of pairings. Indeed the points input into a pairing on a curve of embedding degree k generally take the form $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$. However the twist enables to perform some computations in the sub-field $\mathbb{F}_{q^{k/d'}}$ instead of $\mathbb{F}_{q^k}$, where d' is the degree of the twist. Further, the use of twists can

be use to eliminate the denominator of the function $h_{R,S}$ in the Miller algorithm. Indeed, if we consider the specific case of Weierstrass elliptic curve with a twist of degree d', then if $R = (x_1, y_1)$, $S = (x_2, y_2)$ and $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ we have $h_{R,S}(x, y) := \frac{\ell_{R,S}(x,y)}{d_{R+S}(x,y)} = \frac{ax+by+c}{x-x_3}$ where $a, b, c, x_3 \in \mathbb{F}_q$. Now applying the twist isomorphism defined in proposition 7 page 19 allows us to take the point Q in the form $Q = (x_Q\omega^{-2}, y_Q\omega^{-3})$ with $x_Q, y_Q \in \mathbb{F}_{q^{k/d'}}$ such that :

- For twists of order 2, $h_{R,S}(Q) := \frac{\ell_{R,S}(Q)}{d_{R+S}(Q)} = \frac{(by_Q)\omega+(ax_Q\omega^2+c\omega^4)}{w^2x_Q-x_3\omega^4}$. We can follow the same approach for quartic twists.

- For twists of degree 3 and 6, the equation of the curve is $y^2 = x^3 + b$ such that the denominator of $h_{R,S}$ is $x - x_3 = \frac{y^3-y_3^3}{x^2+x_3x+x_3^2}$. Then a straightforward calculation in the case of twist of order 3 leads to

$$h_{R,S}(Q) := \frac{\ell_{R,S}(Q)}{d_{R+S}(Q)} = \frac{(ax_Q^4\omega^3x_3+by_Qx_Q^2+cx_Q^2\omega^3)\omega^2+(ax_Qx_3^2\omega^6+bx_Qy_Q\omega^3+cx_3\omega^6)\omega+(ax_Q^3\omega^3+by_Qx_3^2\omega^6+cx_3^2\omega^9)}{w^6y_Q^3-y_3^3\omega^9}$$

In all cases, we can easily see that the denominator of $h_{R,S}$ is an element of the sub-field $\mathbb{F}_{q^{k/d'}}$ and because $q^{k/d'} - 1$ divides $q^k - 1$, these denominators are simply equal to 1 in the exponentiation step of the Miller algorithm. So they can be skipped during the algorithm. Moreover all the computations in the numerator of $h_{R,S}$, that is, the evaluation at Q is now done in the sub-field $\mathbb{F}_{q^{k/d'}}$.
Of course we will apply this technique in the next chapter for elliptic curves in Jacobi form.

2. **Extension field arithmetic.** If for the extension field $\mathbb{F}_{q^k}$ the embedding degree has the form $k = 2^a3^b$ then operations in this extension can be performed efficiently since this field can be built up as a tower of extension fields,

$$\mathbb{F}_q \subset \mathbb{F}_{q^{d_1}} \subset \mathbb{F}_{q^{d_2}} \subset \mathbb{F}_{q^{d_1}} \subset \text{.....} \subset \mathbb{F}_{q^{d_k}}$$

where the ith iteration field $\mathbb{F}_{q^i}$ is obtaining by adjoining a root of a polynomial $x^{d_i/d_{i-1}}+\beta_i$ for some $\beta_i \in \mathbb{F}_{q^{d_{i-1}}}$.

3. **Choose r with lower Hamming weight.** In one iteration of Miller's algorithm, if the corresponding bit of r is 1 then we perform the addition and the doubling parts of the algorithm while only the double part is performed if the corresponding bit of r is 0. Then the computation can be done quickly by skipping many addition steps if r has a lower Hamming weight.

1.3.4 Security and efficiency of pairing-based protocols

A pairing-based protocol will be secure if the discrete logarithm problem in the groups $E(\mathbb{F}_q)$ and $\mathbb{F}_{q^k}^\star$ are both computationally infeasible. The best algorithm to solve the discrete logarithm problem in finite field is the index calculus which has subexponential complexity [44] whereas the Pollard rho algorithm [65] is the best algorithm for discrete logarithm computation on elliptic curves with exponential run-time. Therefore the current minimum levels of security required is $r > 2^{160}$ and $q^k > 2^{1024}$. The ratio of these sizes is $\frac{log(q^k)}{log(r)} = k \cdot \rho$. The value ρ measures the base field size relative to the size of the prime-order subgroup on the curve. In general, curves with small ρ values are desirable in order to speed up arithmetic on the elliptic curve. Suitable elliptic curves for pairing-based cryptography are called *pairing-friendly*. The following definition is more precise.

Definition 17. *[30, Definition 2.3] An elliptic curve E defined over a finite field $\mathbb{F}_q$ is called pairing friendly if the two following conditions holds*

1. *There is a prime $r > \sqrt{q}$ dividing $\sharp E(\mathbb{F}_q)$*
2. *The embedding degree of E with respect to r is less than* $\log_2(r)/8$

The paper of Freeman et al. [30] is a good reference to learn about how to generate ordinary elliptic curves suitable for pairing based cryptography. Finally we summarise in table 1.1 the parameters recommended for r and q^k depending on the security level [64].

TABLE 1.1 – Bit sizes of curves parameters and corresponding embedding degrees to obtain commonly desired levels of security.

Security level	Bit length of r	Bit length of q^k	k $\rho \approx 1$	k $\rho \approx 2$
80	160	$960 - 1280$	$6 - 8$	$3 - 4$
128	256	$3000 - 5000$	$12 - 20$	$6 - 10$
192	384	$8000 - 10000$	$20 - 26$	$10 - 13$
256	512	$14000 - 18000$	$28 - 36$	$14 - 18$

The efficient computation of pairings depends in part on the model chosen for the elliptic curve. Pairing computation on the Edwards model of elliptic curves has been done successively in [21, 45] and [1]. The recent results on pairing computation using elliptic curves of Weierstrass form can be found in [18, 19]. Recently in [76], Wang et al. have computed the Tate pairing on Jacobi quartic elliptic curves using the geometric interpretation of the group law. Pairing computation on Hessian form of elliptic curve can be found in [37] and in [80] for Selmer model for elliptic curves.

Chapitre DEUX

Tate pairing computation on elliptic curves of Jacobi forms

In this chapter, we focus on the computation of the Tate Pairing on Jacobi intersection curves and the special Jacobi quartic elliptic curves $Y^2 = dX^4 + Z^4$ over fields of large characteristic p not congruent to 3 modulo 4.
We use the geometric interpretation of the group law of Jacobi intersection curves to obtain the first explicit formulas for the Miller function in Tate pairing computation in this case. For pairing computation with even embedding degree, we define and use the quadratic twist of this curve to obtain efficient formulas in the doubling and addition stages in Miller's algorithm. Moreover, for pairing computation with embedding degree divisible by 4 on the special Jacobi quartic elliptic curve $Y^2 = dX^4 + Z^4$, we define and use its quartic twist to obtain a competitive result with respect to Weierstrass curves [19]. Our result is at the same time an improvement of a previous result on this curve [76] and is therefore, to our knowledge, the best result to date on pairings computation among all curves with quartic twists. The results of this chapter constituted an article with S. Duquesne [26]
The chapter is divided into three sections : In section 2.1, we first look for Miller's function on Jacobi intersection curves using the geometric interpretation of the group law and then compute the Tate pairing on this curve. Section 2.2 presents the computation of the Tate pairing on the Jacobi quartic curve mentioned above using an isomorphism with Weierstrass curves. Finally we use a pairing friendly curve to implement our result in section 2.3.

2.1 Pairing on Jacobi intersection curves

2.1.1 The Jacobi intersection curves

An elliptic curve in Jacobi intersection form over a non binary field $\mathbb{F}_q$ is defined by

$$E_a : \begin{cases} x^2 + y^2 = 1 \\ ax^2 + z^2 = 1 \end{cases} \quad \text{where } a \text{ belongs to } \mathbb{F}_q \text{ and } a(a-1) \neq 0.$$

The Jacobi intersection curve E_a is isomorphic to an elliptic curve in the Weierstrass form $y^2 = x(x-1)(x-a)$. The affine version of the unified addition formulas is given in [15] by $(x_3, y_3, z_3) = (x_1, y_1, z_1) + (x_2, y_2, z_2)$ such that :

$$x_3 = \frac{x_1y_2z_2 + y_1z_1x_2}{y_2^2 + z_1^2x_2^2}, y_3 = \frac{y_1y_2 - x_1z_1x_2z_2}{y_2^2 + z_1^2x_2^2}, z_3 = \frac{z_1z_2 - ax_1y_1x_2y_2}{y_2^2 + z_1^2x_2^2}$$

See [15, 29] for further results on Jacobi intersection curves. An affine point (x, y, z) on a Jacobi intersection curves is represented by the projective homogeneous coordinates (X : Y : Z : T) satisfying

$$\begin{cases} X^2 + Y^2 = T^2 \\ aX^2 + Z^2 = T^2 \end{cases}$$

and $(x, y, z) = (X/T, Y/T, Z/T)$ with $T \neq 0$. The negative of $(X : Y : Z : T)$ is $(-X : Y : Z : T)$. The neutral element $P_0 = (0, 1, 1)$ is represented by $(0 : 1 : 1 : 1)$. By setting $T = 0$ we get four points at infinity : $\Omega_1 = (1 : s : t : 0)$, $\Omega_2 = (1 : s : -t : 0)$, $\Omega_3 = (1 : -s : t : 0)$ and $\Omega_4 = (1 : -s : -t : 0)$ where $1 + s^2 = 0$ and $a + t^2 = 0$.

2.1.2 Efficient group law on Jacobi intersection curves.

The first formulas for addition law on points of Jacobi intersection curves given by Chudnovsky and Chudnovsky in [15] used projective homogeneous coordinates. In [41], Hisil et al. improved these formulas by representing points as a sextuplet $(X : Y : Z : T : XY : ZT)$ as follows :
The sum of the points represented by $(X_1 : Y_1 : Z_1 : T_1 : U_1 : V_1)$ and $(X_2 : Y_2 : Z_2 : T_2 : U_2 : V_2)$ where $U_1 = X_1Y_1$; $V_1 = Z_1T_1$ and $U_2 = X_2Y_2$; $V_2 = Z_2T_2$ is the point $(X_3 : Y_3 : Z_3 : T_3 : U_3 : V_3)$ such that :

$$\begin{aligned} X_3 &= X_1T_1Y_2Z_2 + Y_1Z_1X_2T_2, \\ Y_3 &= Y_1T_1Y_2T_2 - X_1Z_1X_2Z_2, \\ Z_3 &= Z_1T_1Z_2T_2 - aX_1Y_1X_2Y_2, \\ T_3 &= T_1^2Y_2^2 + Z_1^2X_2^2, \\ U_3 &= X_3Y_3, \\ V_3 &= Z_3T_3. \end{aligned}$$

with the algorithm :
$E := X_1Z_2; F := Y_1T_2; G := Z_1X_2; H := T_1Y_2; J := U_1V_2; K := V_1U_2;$
$X_3 := (H + F)(E + G) - J - K; Y_3 := (H + E)(F - G) - J + K;$
$Z_3 := (V_1 - aU_1)(U_2 + V_2) + aJ - K; T_3 := (H + G)^2 - 2K; U_3 := X_3Y_3; V_3 := Z_3T_3.$
This point addition costs $11m_1 + 1s_1 + 2mc$.

The doubling of the point represented by $(X_1 : Y_1 : Z_1 : T_1 : U_1 : V_1)$ is the point $(X_3 : Y_3 : Z_3 : T_3 : U_3 : V_3)$ such that :

$$\begin{aligned} X_3 &= 2X_1Y_1Z_1T_1, \\ Y_3 &= -Z_1^2T_1^2 - aX_1^2Y_1^2 + 2(X_1^2Y_1^2 + Y_1^4), \\ Z_3 &= Z_1^2T_1^2 - aX_1^2Y_1^2, \\ T_3 &= Z_1^2T_1^2 + aX_1^2Y_1^2, \\ U_3 &= X_3Y_3, \\ V_3 &= Z_3T_3. \end{aligned}$$

with the algorithm : $E := V_1^2; F := U_1^2; G := aF; T_3 := E + G; Z_3 := E - G; Y_3 := 2(F + Y_1^4) - T_3; X_3 := (U_1 + V_1)^2 - E - F; U_3 := X_3Y_3; V_3 := Z_3T_3$.
This point doubling costs $2m_1 + 5s_1 + 1mc$.
We present a verification script in the Sage computer algebra system [72] in appendix .1.

2.1.3 Quadratic twist of Jacobi intersection curves.

Proposition 9. *Let the Jacobi intersection curve E_a defined as in section 2.1.1. A quadratic $(t = 2)$ twist of E_a over the extension $\mathbb{F}_{q^{k/2}}$ of $\mathbb{F}_q$ (k even) is the curve*

$$\begin{cases} \delta^2x^2 + y^2 = 1 \\ a\delta^2x^2 + z^2 = 1 \end{cases}$$

Where $\{1, \delta\}$ is the basis of $\mathbb{F}_{q^k}$ as a $\mathbb{F}_{q^{k/2}}$-vector space and $\delta^2 \in \mathbb{F}_{q^{k/2}}$.

Proposition 10. *Let $E_{a,\delta}$ over $\mathbb{F}_{q^{k/2}}$ be a quadratic twist of E_a. The $\mathbb{F}_{q^k}$ isomorphism between $E_{a,\delta}$ and E_a is given by*

$$\begin{array}{rccc} \psi : & E_{a,\delta} & \to & E_a \\ & (x, y, z) & \mapsto & (\delta x, y, z) \end{array}$$

2.1.4 Geometric interpretation of the group law

The aim of this section is to find the function h_{P_1,P_2} with divisor $\mathrm{Div}(h_{P_1,P_2}) = (P_1) + (P_2) - (P_1 + P_2) - (P_0)$. For this, we provide more details to the geometric interpretation of the group law : Three points P_1, P_2, P_3 of the curve will sum to zero if and only if the four points P_0, P_1, P_2, P_3 are coplanar. The negation of a point P_1 is given as the residual intersection of the plane through P_1 containing the tangent line to the curve at P_0. See [56] for more details. Let $\mathcal{P} : f_{P_1,P_2}(x, y, z) = 0$ be the equation of the plane defined by the points P_1, P_2 and P_0. If $P_1 = P_2$ take f_{P_1,P_1} to be the tangent plane to the curve at P_1 passing through P_0. The plane

$\mathcal{P}$ intersects E_a at $-(P_1+P_2)=-P_3$. Then $\mathrm{Div}(f_{P_1,P_2})=(P_1)+(P_2)+(-P_3)+(P_0)-(\Omega)$ where $\Omega=(\Omega_1)+(\Omega_2)+(\Omega_3)+(\Omega_4)$ is a rational divisor.
Let $\mathcal{P}' : g_{P_3}(x,y,z)=0$ be the equation of the plane passing through $-P_3$ and containing the tangent line to the curve at P_0. The plane $\mathcal{P}'$ intersects the curve E_a at the point P_3. Then $\mathrm{Div}(g_{P_3})=(P_3)+2(P_0)+(-P_3)-(\Omega)$. Define

$$h_{P_1,P_2}=\frac{f_{P_1,P_2}}{g_{P_3}}$$

then

$$\mathrm{Div}(h_{P_1,P_2})=(P_1)+(P_2)-(P_1+P_2)-(P_0)$$

Theorem 11. *The functions f_{P_1,P_2} and g_{P_3} are defined as follows :*

$$f_{P_1,P_2}(x,y,z)=\alpha x+\beta(y-1)+\gamma(z-1)$$

with :

$$\begin{aligned}
\alpha &= \begin{cases} (z_2-1)(y_1-1)-(y_2-1)(z_1-1) & if P_1\neq P_2, \\ x_1(-a(y_1-1)+z_1-1) & if P_1=P_2. \end{cases} \\
\beta &= \begin{cases} x_2(z_1-1)-x_1(z_2-1) & if P_1\neq P_2, \\ y_1(z_1-1) & if P_1=P_2 \end{cases} \\
\gamma &= \begin{cases} x_1(y_2-1)-x_2(y_1-1) & if P_1\neq P_2, \\ -z_1(y_1-1) & if P_1=P_2. \end{cases}
\end{aligned}$$

and

$$g_{P_3}(x,y,z)=(z_3-1)(y-1)+(1-y_3)(z-1).$$

Proof 1. .
1. Let $f_{P_1,P_2}(x,y,z)=\alpha x+\beta y+\gamma z+\theta=0$ be the equation of the plane $\mathcal{P}$. Because $P_0=(0,1,1)\in\mathcal{P}$ we have $\theta=-\beta-\gamma$. Thus $f_{P_1,P_2}(x,y,z)=\alpha x+\beta y+\gamma z-\beta-\gamma$.
If P_1 and P_2 are different then by evaluating the previous equation at the points P_1 and P_2 we obtain two linear equations in α, β and γ :

$$\alpha x_1+\beta(y_1-1)+\gamma(z_1-1)=0$$

$$\alpha x_2+\beta(y_2-1)+\gamma(z_2-1)=0$$

with the solutions

$$\alpha=\begin{vmatrix} y_1-1 & z_1-1 \\ y_2-1 & z_2-1 \end{vmatrix},\ \beta=\begin{vmatrix} z_1-1 & x_1 \\ z_2-1 & x_2 \end{vmatrix},\ \gamma=\begin{vmatrix} x_1 & y_1-1 \\ x_2 & y_2-1 \end{vmatrix}$$

If $P_1 = P_2 \neq P_0$ then the tangent line to the curve at P_1 is collinear to the vector $(y_1z_1, -x_1z_1, -ax_1y_1) = (x_1, y_1, 0)\wedge(ax_1, 0, z_1)$. Thus one can take $x_1(-a(y_1-1)+z_1-1), y_1(z_1-1), -z_1(y_1-1)) = (\alpha, \beta, \gamma)$ as a normal vector to the plane.
2. Assume that $\mathcal{P}' : g_{P_3}(x, y, z) = ax + by + cz + d = 0$ and $P_3 = (x_3, y_3, z_3)$. The tangent line to the curve at P_0 is the intersection of the planes $y = 1$ and $z = 1$. Thus P_0 and one arbitrary point $(1, 1, 1)$ on the line belong to the plane $\mathcal{P}'$. This implies that $a = 0$ and $b = -c - d$ such that $g_{P_3}(x, y, z) = c(-y+z)+d(-y+1)$. Because $P_3 = (x_3, y_3, z_3)$ belongs to the plane, we have $c = d(-y_3+1)/(y_3 - z_3)$ and by replacing this value of c in $g_{P_3}(x, y, z) = c(-y+z)+d(-y+1)$ we obtain the desired result.

2.1.5 The Miller function on Jacobi intersection curves

In this section, we show how to use the geometric interpretation of the group law to compute pairings. We assume that k is even. Let $(x_Q, y_Q, z_Q) \in E_{a,\delta}(\mathbb{F}_{q^{k/2}})$. Twisting (x_Q, y_Q, z_Q) with δ ensures that the second argument of the pairing is on $E_a(\mathbb{F}_{q^k})$ and is of the form $Q = (\delta x_Q, y_Q, z_Q)$, where x_Q, y_Q and z_Q are in $\mathbb{F}_{q^{k/2}}$. Since the point Q is fixed during the addition and the doubling step in Miller algorithm, it will be maintained in affine coordinates.

Addition step : $P_1 + P_2 = P_3$. By theorem 11,

$$\begin{aligned} h_{P_1,P_2}(\delta x_Q, y_Q, z_Q) &= \frac{\alpha x_Q\delta + \beta(y_Q - 1) + \gamma(z_Q - 1)}{(z_3 - 1)y_Q + (1 - y_3)z_Q + (y_3 - z_3)} \\ &= \frac{z_Q - 1}{(z_3 - 1)y_Q + (1 - y_3)z_Q + (y_3 - z_3)} \left(\alpha\frac{x_Q}{z_Q - 1}\delta + \beta\frac{y_Q - 1}{z_Q - 1} + \gamma\right) \end{aligned}$$

To obtain the expression of this function in projective coordinates X, Y, Z and T, we set $x_i = \frac{X_i}{T_i}$, $y_i = \frac{Y_i}{T_i}$ and $z_i = \frac{Z_i}{T_i}$; $i = 1, 2, 3$. The function becomes :

$$\begin{aligned} h_{P_1,P_2}(\delta x_Q, y_Q, z_Q) &= \frac{T_3(z_Q - 1)\left(\alpha'\frac{x_Q}{z_Q - 1}\delta + \beta'\frac{y_Q - 1}{z_Q - 1} + \gamma'\right)}{T_1T_2\left[(Z_3 - T_3)y_Q + (T_3 - Y_3)z_Q + (Y_3 - Z_3)\right]} \\ &= \frac{T_3(z_Q - 1)\left(\alpha' M_1\delta + \beta' N_1 + \gamma'\right)}{T_1T_2\left[(Z_3 - T_3)y_Q + (T_3 - Y_3)z_Q + (Y_3 - Z_3)\right]} \end{aligned}$$

where the homogeneous equivalents α', β' and γ' of α, β and γ are

$$\begin{aligned} \alpha' &= (Z_2 - T_2)(Y_1 - T_1) - (Y_2 - T_2)(Z_1 - T_1) \\ \beta' &= X_2(Z_1 - T_1) - X_1(Z_2 - T_2) \\ \gamma' &= X_1(Y_2 - Z_2) - X_2(Y_1 - T_1) \end{aligned}$$

$M_1 = \frac{x_Q}{z_Q - 1}$, $N_1 = \frac{y_Q - 1}{z_Q - 1}$. Observe that $\dfrac{T_3(z_Q - 1)}{T_1T_2[(Z_3 - T_3)y_Q + (T_3 - Y_3)z_Q + (Y_3 - Z_3)]} \in \mathbb{F}_{q^{k/2}}$ so it can be discarded in pairing computation since the final output of Miller loop is raised to the

power $(q^k-1)/r$ and $q^{k/2}-1$ is a factor of $(q^k-1)/r$ since k is even. Thus we only have to evaluate

$$(\alpha' M_1)\delta + \beta' N_1 + \gamma'$$

Since $Q=(\delta x_Q, y_Q, z_Q)$ is fixed during pairing computation, the quantities M_1 and N_1 can be precomputed in $\mathbb{F}_{q^{k/2}}$. Each of the multiplication of α' by $M_1 \in \mathbb{F}_{q^{k/2}}$ and β' by $N_1 \in \mathbb{F}_{q^{k/2}}$ costs $\frac{k}{2}m_1$. Computing the coefficients α', β' and γ' requires $6m_1$ and the point addition in subsection 2.1.1 requires $11m_1+1s_1+2mc$. Thus the point addition and Miller value computation require a total of $1m_k+(k+17)m_1+1s_1+2mc$. The point P_2 is not changed during pairing computation (it is considered as a base point in Miller's algorithm) and can be given in affine coordinates i.e. $T_2=1$. Applying such a mixed addition reduces the cost to $1m_k+(k+16)m_1+1s_1+2mc$.

Doubling step : $2P_1=P_3$. By theorem 11,

$$\begin{array}{l} h_{P_1,P_1}(\delta x_Q, y_Q, z_Q) = \\ \dfrac{x_1(-a(y_1-1)+z_1-1)x_Q\delta + y_1(z_1-1)(y_Q-1) - z_1(y_1-1)(z_Q-1)}{(z_3-1)y_Q+(1-y_3)z_Q+(y_3-z_3)} = \\ \dfrac{x_1(-a(y_1-1)+z_1-1)x_Q\delta + y_1(z_1-1)(y_Q-1) - z_1(y_1-1)(z_Q-1)}{(z_3-1)y_Q+(1-y_3)z_Q+(y_3-z_3)} = \\ \dfrac{(z_Q-1)(x_1(-a(y_1-1)+z_1-1))\dfrac{x_Q}{z_Q-1}\delta + y_1(z_1-1)\dfrac{y_Q}{z_Q-1} - z_1(y_1-1)}{(z_3-1)y_Q+(1-y_3)z_Q+(y_3-z_3)} \end{array}$$

In projective coordinates the function becomes :

$$\begin{array}{rcl} h_{P_1,P_1}(\delta x_Q, y_Q, z_Q) & = & \dfrac{T_3(z_Q-1)\left(\alpha'_1\dfrac{x_Q}{z_Q-1}\delta + \beta'_1\dfrac{y_Q}{z_Q-1} - \gamma'_1)\right)}{T_1^3[(Z_3-T_3)y_Q+(T_3-Y_3)z_Q+(Y_3-Z_3)]} \\ & = & \dfrac{T_3(z_Q-1)}{T_1^3[(Z_3-T_3)y_Q+(T_3-Y_3)z_Q+(Y_3-Z_3)]}(\alpha'_1 M_2\delta + \beta'_1 N_2 - \gamma'_1) \end{array}.$$

Where the homogeneous equivalents α', β' and γ' of α, β and γ are

$$\begin{array}{rcl} \alpha'_1 & = & X_1(-a(Y_1-T_1)+Z_1-T_1) \\ \beta'_1 & = & Y_1(Z_1-T_1) \\ \gamma'_1 & = & Z_1(Y_1-T_1) \end{array}$$

$M_2 = 2a\dfrac{x_Q}{z_Q-1}$ and $N_2 = a\dfrac{y_Q}{z_Q-1}$.The fact that $\dfrac{T_3(z_Q-1)}{T_1^3[(Z_3-T_3)y_Q+(T_3-Y_3)z_Q+(Y_3-Z_3)]} \in \mathbb{F}_{q^{k/2}}$ is not difficult to see, such that this term can be discarded thanks to the final exponentiation. Thus we only have to evaluate

$$(\alpha'_1 M_2)\delta + \beta'_1 N_2 - \gamma'_1$$

Again the quantities M_2 and N_2 are precomputed in $\mathbb{F}_{q^{k/2}}$. Note that each of the multiplications $\alpha_1' M_2$ and $\beta_1' N_2$ costs $\frac{k}{2}m_1$. Computing α_1',β_1' and γ_1' requires $3m_1$ and the point doubling from subsection 2.1.1 requires $2m_1+5s_1+1mc$. Thus the point doubling and Miller value computation require a total of $1m_k + 1s_k + (k+5)m_1 + 5s_1 + 1mc$.

2.1.6 Comparison of results

In this section we confront our results to other results in Tate pairing computation on curves with a quadratic twist. The comparison of results is given in table 2.1. This comparison show

TABLE 2.1 – Comparisons of our pairing formulas with the previous fastest formulas.

Curves	Doubling	Mixed Addition
Weierstrass(a=0)[19]	$1m_k + 1s_k + (k+2)m_1 + 7s_1 + 1mc$	$1m_k + (k+10)m_1 + 2s_1$
Twisted Edwards [1]	$1m_k + 1s_k + (k+6)m_1 + 5s_1 + 2mc$	$1m_k + (k+12)m_1 + 1m_a$
Jacobi quartic[76]	$1m_k + 1s_k + (k+4)m_1 + 8s_1 + 1mc$	$1m_k + (k+16)m_1 + 1s_1 + 4mc$
This work	$1m_k + 1s_k + (k+5)m_1 + 5s_1 + 1mc$	$1m_k + (k+16)m_1 + 1s_1 + 2mc$

that our formulas in Tate pairing computation on Jacobi intersection curves are efficient and competitive with others in the literature, but not significantly better.

2.2 Tate pairing computation on $E_d : Y^2 = dX^4 + Z^4$

2.2.1 The Jacobi quartic curve

A Jacobi quartic elliptic curve over a finite field $\mathbb{F}_q$ is defined by an equation

$$E_{d,\alpha} : y^2 = dx^4 + 2\alpha x^2 + 1$$

with discriminant $\triangle = 256d(\alpha^2 - d)^2 \neq 0$. In [9] Billet and Joye proved that if $E : y^2 = x^3 + ax + b$ has a rational point of order 2 denoted $(\theta, 0)$ then E is bi-rationally equivalent to the Jacobi quartic :

$$Y^2 = dX^4 - 2\delta X^2 Z^2 + Z^4$$

where $d = -(3\theta^2 + 4a)/16$ and $\delta = 3\theta/4$. In the remainder of this section, we will focus our interest on the special Jacobi quartic curve $E_d : Y^2 = dX^4 + Z^4$ because this curve has interesting properties such as quartic twist which contribute to an efficient computation of pairing. The affine model of this curve is $y^2 = dx^4 + 1$ with $(x, y) = (\frac{X}{Z}, \frac{Y}{Z^2})$.

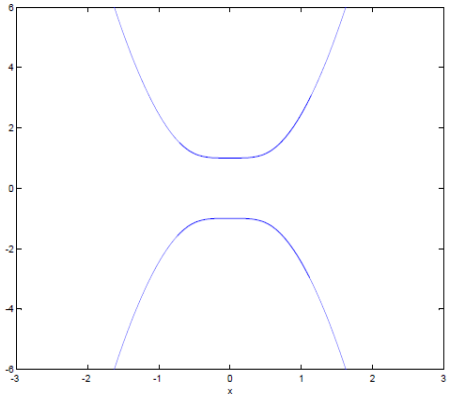

FIGURE 2.1 – The Jacobi quartic $y^2 = 5x^4 + 1$ over $\mathbb{R}$.

The special Jacobi quartic curve E_d is birationally equivalent to the Weierstrass curve $E : y^2 = x^3 - 4dx$ using the maps

$$\varphi \begin{cases} (0:1:1) \longmapsto O \\ (0:-1:1) \longmapsto (0,0) \\ (X:Y:Z) \longmapsto \left(2\frac{(Y+Z^2)}{X^2}, 4\frac{Z(Y+Z^2)}{X^3}\right) \end{cases} ; \varphi^{-1} \begin{cases} O \longmapsto (0:1:1) \\ (0,0) \longmapsto (0:-1:1) \\ (x,y) \longmapsto (2x : 2x^3 - y^2 : y) \end{cases}$$

2.2.2 Group law on the curve $Y^2 = dX^4 + Z^4$.

Here we specialise formulas for point doubling and point addition on the curve E_d from the formulas on the affine model given in [42]. The formulas obtained are news and will enable us, together with pairings formulas, to obtain efficient results in the computation of pairings. The point addition $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ on the affine model of E_d is given by :

$$x_3 = \frac{x_1^2 - x_2^2}{x_1y_2 - y_1x_2}, \qquad y_3 = \frac{(x_1 - x_2)^2}{(x_1y_2 - y_1x_2)^2}(y_1y_2 + 1 + dx_1^2x_2^2) - 1.$$

By replacing x_1 by $\frac{X_1}{Z_1}$, x_2 by $\frac{X_2}{Z_2}$, y_1 by $\frac{Y_1}{Z_1^2}$, y_2 by $\frac{Y_2}{Z_2^2}$, $x_3 = \frac{X_3}{Z_3}$ and y_3 by $\frac{Y_3}{Z_3^2}$ a simple calculation yields to

$$\begin{aligned} X_3 &= X_1^2Z_2^2 - Z_1^2X_2^2 \\ Z_3 &= X_1Z_1Y_2 - X_2Z_2Y_1 \\ Y_3 &= (X_1Z_2 - X_2Z_1)^2(Y_1Y_2 + (Z_1Z_2)^2 + d(X_1X_2)^2) - Z_3^2 \end{aligned}$$

The point doubling $(x_3, y_3) = 2(x_1, y_1)$ on the affine model of E_d is given by :

$$x_3 = \frac{2y_1}{2 - y_1^2}x_1, \qquad y_3 = \frac{2y_1}{2 - y_1^2}\left(\frac{2y_1}{2 - y_1^2} - y_1\right) - 1.$$

By replacing x_1 by $\frac{X_1}{Z_1}$, y_1 by $\frac{Y_1}{Z_1^2}$, x_3 by $\frac{X_3}{Z_3}$ and y_3 by $\frac{Y_3}{Z_3^2}$, a simple calculation yields to :

$$\begin{aligned} X_3 &= 2X_1Y_1Z_1 \\ Z_3 &= Z_1^4 - dX_1^4 \\ Y_3 &= 2Y_1^4 - Z_3^2 \end{aligned}$$

We present a verification script in the Sage computer algebra system [72] in appendix .2.

2.2.3 Quartic twists of Jacobi quartic curves

To obtain the twist of the Jacobi quartic curve defined by $Y^2 = dX^4 + Z^4$, we use the bi-rational maps defined in section 2.2.1 and the twist of Weierstrass curves defined in proposition 7 page 19. We assume that k is divisible by 4.

Proposition 11. *A quartic twist of the Jacobi quartic curve $Y^2 = dX^4 + Z^4$ over the extension $\mathbb{F}_{q^{k/4}}$ of $\mathbb{F}_q$ is the curve*

$$E_{d,\omega} : Y^2 = d\omega^4 X^4 + Z^4$$

where $\omega \in \mathbb{F}_{q^k}$ is such that $\omega^2 \in \mathbb{F}_{q^{k/2}}$, $\omega^3 \in \mathbb{F}_{q^k} \backslash \mathbb{F}_{q^{k/2}}$ and $\omega^4 \in \mathbb{F}_{q^{k/4}}$.
That is $\{1, \omega, \omega^2, \omega^3\}$ is a basis of $\mathbb{F}_{q^k}$ as a vector space over $\mathbb{F}_{q^{k/4}}$.

Proposition 12. *Let $E_{d,\omega}$ over $\mathbb{F}_{q^{k/4}}$ be a twist of E_d. The $\mathbb{F}_{q^k}$ isomorphism between $E_{d,\omega}$ and E_d is given by*

$$\begin{array}{rccc} \psi : & E_{d,\omega} & \to & E_d \\ & (X : Y : Z) & \mapsto & \left(\frac{X}{\omega^2} : \frac{Y}{\omega^6} : \frac{Z}{\omega^3}\right) \end{array}$$

2.2.4 The Miller function

Wang et al. in [76] considered pairings on Jacobi quartics and gave the geometric interpretation of the group law. We use a different way, namely bi-rational equivalence between Jacobi quartic curves and Weierstrass curves, of obtaining the formulas. We specialise to the particular curves $E_d : Y^2 = dX^4 + Z^4$ to obtain better results for these up to 26% improvement compared to results in [76].
Given two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on the Weierstrass curve E such that $P_3 = (x_3, y_3) = P_1 + P_2$, consider $R = (X_1, Y_1, Z_1)$, $S = (X_2, Y_2, Z_2)$ and $(X_3, Y_3, Z_3) = (X_1, Y_1, Z_1) + (X_2, Y_2, Z_2)$ the corresponding points on the jacobi quartic E_d. To derive the Miller function $h_{R,S}(X, Y, Z)$ for E_d, we first write the Miller function $h_{P_1,P_2}(x, y)$ on the Weierstrass

curve E. Then by using the birational equivalence we have $h_{R,S}(X,Y,Z) = h_{P_1,P_2}(\varphi(X,Y,Z))$. The Miller function $h_{P_1,P_2}(x,y)$ for this Weierstrass curve is

$$h_{P_1,P_2}(x,y) = \frac{y - \lambda x - \alpha}{x - x_3}$$

Where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ if $P_1 \neq P_2$ and $\lambda = \dfrac{3x_1^2 - 4d}{2y_1}$ if $P_1 = P_2$ and $\alpha = y_1 - \lambda x_1$. As explained at the beginning of this section, the Miller function for the Jacobi quartic $E_d : Y^2 = dX^4 + Z^4$ is given by $h_{R,S}(X,Y,Z) = h_{P_1,P_2}(\varphi(X,Y,Z))$. We have :

$$h_{R,S}(X,Y,Z) = \frac{4X_3^2X^2}{2X_3^2(Y+Z^2) - 2X^2(Y_3 + Z_3^2)}\left(\frac{ZY + Z^3}{X^3} - \frac{1}{2}\lambda\left(\frac{Y+Z^2}{X^2}\right) - \frac{\alpha}{4}\right)$$

where

$$\lambda = \begin{cases} \dfrac{-2X_1^3Z_2(Y_2+Z_2^2) + 2X_2^3Z_1(Y_1+Z_1^2)}{X_1X_2[-X_1^2(Y_2+Z_2^2) + X_2^2(Y_1+Z_1^2)]} & \text{if } P_1 \neq P_2, \\ \dfrac{Y_1 + 2Z_1^2}{X_1Z_1} & \text{if } P_1 = P_2 \end{cases}$$

and

$$\alpha = \begin{cases} \dfrac{-4(Y_1+Z_1^2)(Y_2+Z_2^2)(Z_2X_1 - Z_1X_2)}{X_1X_2[-X_1^2(Y_2+Z_2^2) + X_2^2(Y_1+Z_1^2)]} & \text{if } P_1 \neq P_2 \\ \dfrac{-2Y_1(Y_1+Z_1^2)}{X_1^3Z_1} & \text{if } P_1 = P_2 \end{cases}$$

Remark 8. *It is simple to verify that our formula obtained by change of variables is exactly the same result obtained by Wang et al. in [76] using the geometric interpretation of the group law.*
Indeed, by setting $x_1 = \frac{X_1}{Z_1}$, $x_2 = \frac{X_2}{Z_2}$, $y_1 = \frac{Y_1}{Z_1^2}$ *and* $y_2 = \frac{Y_2}{Z_2^2}$ *in their Miller function obtained for the curve* $E_{d,a} : y^2 = dx^4 + 2ax + 1$ *(by taking* $a = 0$*), we get exactly the same result that we found above.*

2.2.5 Simplification of the Miller function

By using twist technique as explained earlier, the point Q in the Tate pairing computation can be chosen to be $\left(\frac{X_Q}{\omega^2} : \frac{Y_Q}{\omega^6} : \frac{Z_Q}{\omega^3}\right)$ or $(x_Q\omega, y_Q, 1)$ in affine coordinates where X_Q, Y_Q, Z_Q, x_Q and y_Q are in $\mathbb{F}_{q^{k/4}}$. Thus

$$h_{R,S}(x_Q\omega, y_Q, 1) = \frac{2X_3^2x_Q^2\omega^2}{X_3^2(y_Q+1) - x_Q^2\omega^2(Y_3+Z_3^2)}\left(-\frac{1}{2}\lambda\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)\omega^2 + \left(\frac{y_Q+1}{x_Q^3\omega^4}\right)\omega - \frac{\alpha}{4}\right)$$

Write $-\frac{\alpha}{4} = \frac{A}{D}$ and $-\frac{1}{2}\lambda = \frac{B}{D}$ then

$$h_{R,S}(x_Q\omega, y_Q, 1) = \frac{2X_3^2x_Q^2\omega^2D^{-1}}{X_3^2(y_Q+1) - x_Q^2\omega^2(Y_3+Z_3^2)}\left(B\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)\omega^2 + D\left(\frac{y_Q+1}{x_Q^3\omega^4}\right)\omega + A\right)$$

We can easily see that $\frac{2X_3^2x_Q^2\omega^2}{D(X_3^2(y_Q+1)-x_Q^2\omega^2(Y_3+Z_3^2))} \in \mathbb{F}_{q^{k/2}}$ so it can be discarded in pairing computation thanks to the final exponentiation. Thus we only have to evaluate

$$h_{R,S}(x_Q\omega, y_Q, 1) = B\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)\omega^2 + D\left(\frac{y_Q+1}{x_Q^3\omega^4}\right)\omega + A$$

Since $Q = (x_Q\omega, y_Q, 1)$ is fixed during pairing computation, the quantities $\frac{y_Q+1}{x_Q^3\omega^4}$ and $\frac{y_Q+1}{x_Q^2\omega^4}$ can be precomputed in $\mathbb{F}_{q^{k/4}}$. Note that each of the multiplications $D\left(\frac{y_Q+1}{x_Q^3\omega^4}\right)$ and $B\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)$ costs $\frac{k}{4}m$.

Remark 9. *We can use the fact that in the expression of $h := h_{R,S}$ the term ω^3 is absent and $A \in \mathbb{F}_q$. Thus in Miller's algorithm, the cost of the main multiplication in $\mathbb{F}_{q^k}$ is not $1M$ but $\left(\frac{1}{k} + \frac{1}{2}\right)M$ assuming that schoolbook multiplication is used.*
But if we are using pairing friendly fields, the embedding degree will be of the form $k = 2^i3^j$. Then we follow [49] and the cost of a multiplication or a squaring in the field $\mathbb{F}_{q^k}$ is 3^i5^j multiplications or squaring in $\mathbb{F}_q$ using Karatsuba and multiplication method. In this case, in Miller's algorithm, the cost of the main multiplication in $\mathbb{F}_{q^k}$ is $\left(\frac{7\cdot3^{i-2}5^j+2^{i-2}3^j}{3^i5^j}\right)m_k$. In the next sections λ' stands for $\frac{1}{k} + \frac{1}{2}$ or $\frac{7\cdot3^{i-2}5^j+2^{i-2}3^j}{3^i5^j}$.
Indeed the main multiplication in Miller's algorithm is of the form $f \cdot h$ where f and h are in $\mathbb{F}_{q^k}$. Since $\mathbb{F}_{q^k}$ is a $\mathbb{F}_{q^{k/4}}$-vector space with basis $\{1, \omega, \omega^2, \omega^3\}$, f and h can be written as : $f = f_0 + f_1\omega + f_2\omega^2 + f_3\omega^3$ and $h = h_0 + h_1\omega + h_2\omega^2 + h_3\omega^3$ with f_i and h_i in $\mathbb{F}_{q^{k/4}}$, $i = 0, 1, 2, 3$. However in our case $h_3 = 0$, $h_0 \in \mathbb{F}_q$ and $k = 2^i3^j$.

Schoolbook method : *A full multiplication $f.h$ costs k^2 multiplications in the base field $\mathbb{F}_q$ using schoolbook method. But thanks to the particular form of h_0 and h_3, each of the multiplications $f_i \cdot h_0$ costs $\frac{k}{4}$ and each of the multiplications $f_i \cdot h_1$, $f_i \cdot h_2$ costs $\frac{k^2}{16}$, $i = 0, 1, 2, 3$. Then final cost of the product $f \cdot h$ in the base field $\mathbb{F}_q$ is $8\frac{k^2}{16} + 4\frac{k}{4} = \frac{k^2}{2} + k$. Finally the ratio of the cost in this case by the cost of the general multiplication is $\frac{\frac{k^2}{2}+k}{k^2} = \frac{1}{2} + \frac{1}{k}$.*

Karatsuba method : *The computation of $f \cdot h$ is done by computing the three products : $u = (f_0 + f_1\omega)(h_0 + h_1\omega)$ which costs $2^{i-2}3^j + 2(3^{i-2}5^j)$, $v = (f_2 + f_3\omega)(h_2 + h_3\omega)$ which costs $2(3^{i-2}5^j)$ and $w = (f_0 + f_2 + (f_1 + f_3)\omega)(h_0 + h_2 + (h_1 + h_3)\omega)$ which costs $3(3^{i-2}5^j)$. The final cost is then $7 \cdot 3^{i-2}5^j + 2^{i-2}3^j$.*

In the next sections, we will compute A, B and D. In the work of Hisil et al. [42], there are different formulas in affine version for scalar multiplication. They used one of them to improve point addition and point doubling. These improved formulas have been used by Wang et al. to compute pairings. But in our case we obtained our formulas from a different affine version. For efficiency the point is represented by $(X : Y : Z : X^2 : Z^2)$ with $Z \neq 0$. We present the first time that this representation is used when $d \neq 1$. Thus we will use the points $P_1 = (X_1 : Y_1 : Z_1 : U_1 : V_1)$ and $P_2 = (X_2 : Y_2 : Z_2 : U_2 : V_2)$ where $U_i = X_i^2$, $V_i = Z_i^2$, $i = 1, 2$.

Remark 10. *Note that if X^2 and Z^2 are known then expressions of the form XZ can be computed using the formula $((X+Z)^2 - X^2 - Z^2)/2$. This allows the replacement of a multiplication by a squaring presuming a squaring and three additions are more efficient. The operations concerned with this remark are followed by $*$ in tables 2.3 and 2.2.*

2.2.6 Point doubling and Miller iteration

When $P_1 = P_2$, we have $A = Y_1(Y_1 + Z_1^2)$, $D = 2X_1^3 Z_1$ and $B = -X_1^2(Y_1 + 2Z_1^2)$. The computation of A, B, D and the point doubling can be done using the algorithm in table 2.2 with $4m_1 + 6s_1 + 1mc$ or $3m_1 + 7s_1 + 1mc$ according to the remark 10.

TABLE 2.2 – Combined formulas for doubling and Miller value computation.

Operations		*Values*	*Cost*
$U := U_1^2$		$U = X_1^4$	$1s_1$
$V := V_1^2$		$V = Z_1^4$	$1s_1$
$Z_3 := V - dU$		$Z_3 = Z_1^4 - dX_1^4$	$1m_d$
$E := ((X_1 + Z_1)^2 - U_1 - V_1)/2$	$*$	$E = X_1 Z_1$	$1m_1$ or $1s_1$
$D := 2U_1 E$		$D = 2X_1^3 Z_1$	$1m_1$
$A := (2Y_1 + V_1)^2/4 - U$		$A = Y_1(Y_1 + Z_1^2)$	$1s_1$
$B := -U_1(Y_1 + 2V_1)$		$B = -X_1^2(Y_1 + 2Z_1^2)$	$1m_1$
$X_3 := 2EY_1$		$X_3 = 2X_1 Y_1 Z_1$	$1m_1$
$V_3 := Z_3^2$		$V_3 = Z_3^2$	$1s_1$
$Y_3 := 2V - Z_3$		$Y_3 = dX_1^4 + Z_1^4 = Y_1^2$	-
$Y_3 := 2Y_3^2 - V_3$		$Y_3 = 2Y_1^4 - Z_3^2$	$1s_1$
$U_3 := X_3^2$		$U_3 = X_3^2$	$1s_1$
Total cost : $4m_1 + 6s_1 + 1mc$ or $3m_1 + 7s_1 + 1mc$			

Thus the point doubling and Miller value computation require a total of $\lambda' m_k + 1s_k + (\frac{k}{2} + 4)m_1 + 6s_1 + 1mc$ or $\lambda' m_k + 1s_k + (\frac{k}{2} + 3)m_1 + 7s_1 + 1mc$.

2.2.7 Point addition and Miller iteration

When $P_1 \neq P_2$ we have $A = (Y_1 + Z_1^2)(Y_2 + Z_2^2)(Z_1X_2 - Z_2X_1)$,
$D = X_1X_2[-X_1^2(Y_2 + Z_2^2) + X_2^2(Y_1 + Z_1^2)]$ and $B = X_1^3Z_2(Y_2 + Z_2^2) - X_2^3Z_1(Y_1 + Z_1^2)$.
Using the algorithm in table 2.3 the computation of A, B, D and the point addition can be done in $18m_1 + 5s_1 + 1mc$ or $12m_1 + 11s_1 + 1mc$ according to remark 10. Applying mixed addition($Z_2 = 1$), this cost is reduced to $15m_1 + 4s_1 + 1mc$ or $12m_1 + 7s_1 + 1mc$. Thus the point addition and Miller value computation require a total of $\lambda' m_k + 1s_k + \left(\frac{k}{2} + 15\right) m_1 + 4s_1 + 1mc$ or $\lambda' m_k + 1s_k + \left(\frac{k}{2} + 12\right) m_1 + 7s_1 + 1mc$.

TABLE 2.3 – Combined formulas for addition and Miller value computation.

Operations		*Values*	*Cost*
$U := Y_1 + V_1$		$U = Y_1 + Z_1^2$	-
$V := Y_2 + V_2$		$V = Y_2 + Z_2^2$	-
$R := ((X_1 + Z_2)^2 - U_1 - V_2)/2$	*	$R = Z_2X_1$	$1m_1$
$S := ((X_2 + Z_1)^2 - U_2 - V_1)/2$	*	$S = Z_1X_2$	$1m_1$
$A := S - R$		$A = Z_1X_2 - Z_2X_1$	-
$A := AV$		$A = (Y_2 + Z_2^2)(Z_1X_2 - Z_2X_1)$	$1m_1$
$A := AU$		$A = (Y_1 + Z_1^2)(Y_2 + Z_2^2)(Z_1X_2 - Z_2X_1)$	$1m_1$
$U := U_2U$		$U = X_2^2(Y_1 + Z_1^2)$	-
$V := U_1V$		$V = X_1^2(Y_2 + Z_2^2)$	$1m_1$
$B := RV - SU$		$B = X_1^3Z_2(Y_2 + Z_2^2) - X_2^3Z_1(Y_1 + Z_1^2)$	$2m_1$
$D := ((X_1 + X_2)^2 - U_1 - U_2)/2$	*	$D = X_1X_2$	$1m_1$ or $1s_1$
$E := dD^2$		$E = d(X_1X_2)^2$	$1m_d + 1s_1$
$D := D(U - V)$		$D = X_1X_2[-X_1^2(Y_2 + Z_2^2) + X_2^2(Y_1 + Z_1^2)]$	$1m_1$
$X_3 := (R + S)(R - S)$		$X_3 = X_1^2Z_2^2 - Z_1^2X_2^2$	$1m_1$
$W_1 := ((X_1 + Z_1)^2 - U_1 - V_1)/2$	*	$W_1 = X_1Z_1$	$1m_1$ or $1s_1$
$W_2 := ((X_2 + Z_2)^2 - U_2 - V_2)/2$	*	$W_2 = X_2Z_2$	$1m_1$ or $1s_1$
$Z_3 := W_1Y_2 - W_2Y_1$		$Z_3 = X_1Z_1Y_2 - X_2Z_2Y_1$	$2m_1$
$U := Y_1Y_2$		$U = Y_1Y_2$	$1m_1$
$V := ((Z_1 + Z_2)^2 - V_1 - V_2)/2$	*	$V = Z_1Z_2$	$1m_1$ or $1s_1$
$V := V^2 + E$		$V = (Z_1Z_2)^2 + d(X_1X_2)^2$	$1s_1$
$E := (R - S)^2$		$E = (X_1Z_2 - X_2Z_1)^2$	$1s_1$
$U_3 := X_3^2$		$U_3 = X_3^2$	$1s_1$
$V_3 := Z_3^2$		$V_3 = Z_3^2$	$1s_1$
$Y_3 := E(U + V) - V_3$		$Y_3 = (X_1Z_2 - X_2Z_1)^2(Y_1Y_2 + (Z_1Z_2)^2 +$ $d(X_1X_2)^2) - Z_3^2$	$1m_1$
Total cost : $18m_1 + 5s_1 + 1mc$ or $12m_1 + 11s_1 + 1mc$			

2.2.8 Comparison

The comparison of results is summarized in table 2.4 and table 2.5. These comparisons are made for the Tate pairing and curves with a quartic twist.
In table 2.4, we assume that Schoolbook multiplication method is used. We also present an example of comparison in the cases $k = 8$ since this value is one of the most appropriate for cryptographic applications when a quartic twist is used.

Remark 11. *If we assume that $m_1 = s_1 = mc$ and $k = 8$ then for the doubling step the total*

TABLE 2.4 – Comparison of our pairing formulas with the previous fastest formulas with an example using Schoolbook multiplication method.

Curves	Doubling	Mixed Addition
Weierstrass(b=0)[19]	$1m_k + 1s_k + (\frac{k}{2}+2)m_1 + 8s + 1mc$	$1m_k + (\frac{k}{2}+9)m_1 + 5s_1$
Jacobi quartic(a=0)[76]	$1m_k + 1s_k + (\frac{k}{2}+5)m_1 + 6s_1$	$1m_k + (\frac{k}{2}+16)m_1 + 1s_1 + 1mc$
This work	$(\frac{1}{k}+\frac{1}{2})m_k + 1s_k + (\frac{k}{2}+3)m_1 + 7s_1 + 1mc$	$(\frac{1}{k}+\frac{1}{2})m_k + (\frac{k}{2}+12)m_1 + 7s_1 + 1mc$
Example : $k = 8$		
Weierstrass(b=0)[19]	$98m_1 + 16s_1 + 1mc$	$77m_1 + 5s_1$
Jacobi quartic (a=0)[76]	$101m_1 + 14s_1$	$84m_1 + 1s_1 + 1mc$
This work	$75m_1 + 15s_1 + 1mc$	$57m_1 + 6s_1 + 1mc$

costs are $115m_1$, $115m_1$ *and* $91m_1$ *for Weierstrass curve, Jacobi quartic curve (a=0)[76] and* this work *respectively. Hence, we obtain in this work a theoretical gain of* 21% *with respect to Weierstrass curves and Jacobi quartic curves. Similarly for the addition step we obtain a theoretical gain of* 22% *and* 26% *over Weierstrass and Jacobi quartic curves respectively. This theoretical gain increases together with the value of k, see table 2.4.*

In table 2.5, we present the costs in the case where Karatsuba method is used for curves with $k = 2^i 3^j$. We also present an example of comparison in the cases $k = 8$ and $k = 16$ since these values are the most appropriate for cryptographic applications when a quartic twist is used.

Remark 12. *We assume again that* $m_1 = s_1 = mc$. *For* $k = 8$ *and for the doubling step we obtain a theoretical gain of* 6% *over Weierstrass curves and Jacobi quartic curves (a=0)[76]. This theoretical gain increases together with the value of k. When* $k = 16$ *the gain is* 8% *both for the addition and doubling step over Weierstrass curves. The improvement is* 13% *in addition step over Jacobi quartic curves, see table 2.5.*

Remark 13. *The security and the efficiency of pairing-based systems requires using pairing-friendly curves. The Jacobi models of elliptic curves studied in this work are isomorphic to Weierstrass curves. Thus we can obtain pairing friendly curves of such models using the construction given by Galbraith et al.[33] or by Freeman et al.[30]. Some examples of pairing friendly curves of Jacobi quartic form can be found in [76].*

TABLE 2.5 – Comparison of our pairing formulas with the previous fastest formulas with an example using Karatsuba multiplication method.

Curves	Doubling	Mixed Addition
Weierstrass(b=0)[19]	$1m_k + 1s_k + (\frac{k}{2}+2)m_1 + 8s_1 + 1mc$	$1m_k + (\frac{k}{2}+9)m_1 + 5s_1$
Jacobi quartic(a=0)[76]	$1m_k + 1s_k + (\frac{k}{2}+5)m_1 + 6s_1$	$1m_k + (\frac{k}{2}+16)m_1 + 1s_1 + 1mc$
This work	$\left(\frac{7\cdot 3^{i-2}5^j + 2^{i-2}3^j}{3^i 5^j}\right) m_k + 1s_k + (\frac{k}{2}+3)m_1 + 7s_1 + 1mc$	$\left(\frac{7\cdot 3^{i-2}5^j + 2^{i-2}3^j}{3^i 5^j}\right) m_k + (\frac{k}{2}+12)m_1 + 7s_1 + 1mc$
Example 1 : $k = 8$		
Weierstrass(b=0)[19]	$33m_1 + 35s_1 + 1mc$	$40m_1 + 5s_1$
Jacobi quartic (a=0)[76]	$36m_1 + 33s_1$	$84m_1 + 1s_1 + 1mc$
This work	$30m_1 + 34s_1 + 1mc$	$39m_1 + 7s_1 + 1mc$
Example 2 : $k = 16$		
Weierstrass(b=0)[19]	$91m_1 + 89s_1 + 1mc$	$98m_1 + 5s_1$
Jacobi quartic (a=0)[76]	$94m_1 + 87s_1$	$105m_1 + 1s_1 + 1mc$
This work	$78m_1 + 88s_1 + 1mc$	$87m_1 + 7s_1 + 1mc$

2.3 Implementation of the Tate pairing

In this section we consider the familly of elliptic curves of embedding degree 8 described in [73] to implement the Tate pairing. This familly of curves has the following parameters :

$$\begin{aligned} r &= 82x^4 + 108x^3 + 54x^2 + 12x + 1 \\ p &= 379906x^6 + 799008x^5 + 705346x^4 + 333614x^3 + 88945x^2 + 12636x + 745 \end{aligned}$$

For $x = 24000000000010394$, the values of r, q and the curve coefficient d are :

$$\begin{aligned} r &= 272056320000471307161600306182614014808404525177076771934828454768 17, \\ p &= 726011672004446604951703464791789328991217313776602768811505320697 58156754787842298703647640196322590069, \\ d &= 453757295002779128094814665494868330619510821110376730507190825435988479717424014366897797751227016187 93, \\ t &= -113356800000147285043200063789391713609209096429146 0, \end{aligned}$$

We made implementations with Magma software, V2.15-3, [12] running on a Linux Lubuntu on a 64-bit PC with characteristics 1.00 GHZ and 5 GB of RAM. The code for the implementation of the Tate pairing is given in appendix .3.

Chapitre TROIS

Computation of Ate pairing and its variations on the Jacobi quartic elliptic curve $Y^2 = dX^4 + Z^4$

Since the development of pairing-based cryptography, the efficiency of the Miller algorithm, the main tool in pairing computation, has been successfully improved. One way to do this is based on shortening the loop length in this algorithm that leads, in addition to Weil and Tate pairings, to other pairings such as : -the Eta-pairing [4] on certain supersingular elliptic curves, - Ate and twisted Ate pairings that are closely related to the Eta-pairing but can be used efficiently with ordinary elliptic curves introduced in [40]. In [74], Vercauteren introduced the concept of optimal pairings that can be computed using the smallest number of basic Miller's iterations. The computation of these different pairings has been done by Costello et al. in [19] in the case of Weierstrass curves.
In the previous chapter, a portion was devoted to the computation of the Tate pairing on the Jacobi quartic $Y^2 = dX^4 + Z^4$. In this chapter, we extend these results to Ate pairing and its variations, namely the twisted Ate and optimal pairings. Our results show that among known curves with quartic twists, the Jacobi model $Y^2 = dX^4 + Z^4$ offers the best performances for these different pairings. The chapter is divided as follows : The first section introduces Ate pairing and its variations. In section 3.2, we determine the Miller function and rewrite the addition formulas for Ate pairing. Section 3.2.4 is devoted to a comparative study of these pairings on the curves of Jacobi and Weierstrass forms. Section 3.3, we generate a pairing friendly curve of this Jacobi form to implement both Ate and the optimal pairings.

3.1 Ate pairing and its variations

In this section, we briefly define Ate pairing and the twisted Ate pairing. The results in this section are very well described in the original article of Hess et al. [40]. Let E be an elliptic curve over a finite field $\mathbb{F}_q$, r a large prime such that $r \mid \sharp E(\mathbb{F}_q)$ and let k be the embedding

degree of E with respect to r. The set of $r-$th roots of unity in $\mathbb{F}_{q^k}^\star$ is denoted μ_r. We recall that $f_{n,R}$ the function with divisor

$$\mathrm{Div}(f_{n,R}) = n(P) - n(P_0)$$

Let π_q be the Frobenius endomorphism defined in proposition 4 page 17. Denote t the trace of the Frobenius. By using propositions 3 and 4 and the fact that π_q satisfies it characteristic polynomial (Cayley Hamilton theorem), we have the following equality :

$$\pi_q^2 - t\pi_q + q = 0$$

The relation between the trace t of the Frobenius endomorphism and the group order is given by [77, Theorem 4.3] :

$$\sharp E(\mathbb{F}_q) = q + 1 - t$$

The Frobenius endomorphism π_q has exactly two eigenvalues. Indeed, using the Lagrange theorem in the multiplicative group $(\mathbb{F}_q^\star, \times)$, it is clear that 1 is an eigenvalue. We then use the characteristic polynomial to conclude that q is the other one. This enables to consider $P \in \mathbb{G}_1 = E(\overline{\mathbb{F}_q})[r] \cap \mathrm{Ker}(\pi_q - [1]) = E(\mathbb{F}_q)[r]$ and $Q \in \mathbb{G}_2 = E(\overline{\mathbb{F}_q})[r] \cap \mathrm{Ker}(\pi_q - [q])$.

Ate pairing

Definition 18. *(Ate pairing) The reduced Ate pairing is the map defined as follows :*

$$\begin{array}{rccc} e_A : & \mathbb{G}_2 \times \mathbb{G}_1 & \to & \mu_r \\ & (Q, P) & \mapsto & f_{T,Q}(P)^{\frac{q^k-1}{r}} \end{array}$$

where $T = t - 1$.

The following theorem gives some properties of Ate pairing, in particular its relation with the Tate pairing. This relation makes sense to definition 18 : Ate pairing is a power of the Tate pairing and therefore is a pairing.

Theorem 12. *[40] Let* $N = gcd(T^k - 1, q^k - 1)$ *and* $T^k - 1 = LN$. *We have*

- $e_T(Q, P)^{LN} = e_A(Q, P)^{rc}$ *where* $e_T(Q, P)$ *is the Tate pairing and where* $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \mod r$.
- *for* $r \nmid L$, *Ate pairing* e_A *is non-degenerate.*

Indeed the choice of $\mathbb{G}_1$ and $\mathbb{G}_2$ allows to show that Ate pairing is a power of the Tate pairing. The condition $N = gcd(T^k - 1, q^k - 1)$ ensures that N is a multiple of r which divides $q^k - 1$. In fact observe that since r is a divisor of $\sharp E(\mathbb{F}_q) = q - T$ we have $q \equiv T \mod r$,

which implies that $q^k \equiv T^k \bmod r$. so r divides $T^k - 1$ and $q^k - 1$ and thus is a divisor of N, the greatest common divisor of $T^k - 1$ and $q^k - 1$. Thus we have $f_{N,Q}(P)^{\frac{q^k-1}{N}} = f_{r,Q}(P)^{\frac{q^k-1}{r}}$ by proposition 8 page 21. Observe that up to power $\frac{q^k-1}{N}$ the functions $f^L_{N,Q}$ and $f_{LN,Q}$ are equal since they have the same divisors such that $f_{N,Q}(P)^{\frac{q^k-1}{N}} = e_T(Q,P)$. Raising to the power LN we obtain $e_T(Q,P)^{LN} = f_{LN,Q}(P)^{(q^k-1)} = f_{T^k-1,Q}(P)^{(q^k-1)} = f_{T^k,Q}(P)^{(q^k-1)}$. The last equality is true because $T^kQ = Q$. Now because $f_{ij,Q} = f^j_{i,Q} f_{j,iQ} = f^i_{j,Q} f_{i,jQ}$, $Q \in \mathrm{Ker}(\pi_q - [q])$, $q \equiv T \bmod r$ and $f_{T,T^iQ}(P) = f_{T,\pi^i_q(Q)}(P) = \pi^i_q(f_{T,Q}(P)) = f_{T,Q}(P)^{q^i}$, we have $f_{T^k,Q}(P)^{L(q^k-1)} = f_{T,Q}(P)^{T^{k-1}} \times f_{T,TQ}(P)^{T^{k-2}} \times \ldots\ldots \times f_{T,T^{k-1}Q}(P) = f_{T,Q}(P)^{T^{k-1}} \times f_{T,Q}(P)^{T^{k-2}q} \times \ldots\ldots \times f^{q^{k-1}}_{T,Q}(P)$ $= f^c_{T,Q}(P)$ where $c = \sum_{i=0}^{k-1} T^{k-1-i}q^i \equiv \sum_{i=0}^{k-1} q^{k-1-i}q^i \equiv kq^{k-1} \bmod r$. Now we can write $N = rs$ for some integer r such that $e_T(Q,P)^{Lsc^{-1}} = e_A(Q,P)$. A more comprehensive proof can be found in [40].

Remark 14. *The Tate pairing is defined on $\mathbb{G}_1 \times E(\mathbb{F}_{q^k})$, while Ate pairing is defined on $\mathbb{G}_2 \times \mathbb{G}_1$ with $\mathbb{G}_2 \subseteq E(\mathbb{F}_{q^k})$. This means that during the execution of the Miller algorithm in Ate pairing computation, the point addition is performed in an extension field of $\mathbb{F}_q$ whereas it was performed in $\mathbb{F}_q$ in the case of the Tate pairing. As the arithmetic over $\mathbb{F}_{q^k}$ is much more expensive than the arithmetic over $\mathbb{F}_q$, each step of Ate pairing is more expensive than the Tate pairing. However the Miller loop length in the case of Ate pairing is $\log_2(T)$ which is less (generally the half) than $\log_2(r)$, the loop length for the Tate pairing.*

Observe that if Ate pairing were defined on $\mathbb{G}_1 \times \mathbb{G}_2$, then it will be faster than the Tate pairing since its Miller loop length will be approximately halved. This remark yields to the definition of the twisted Ate pairing [40].

Definition 19. *(The twisted Ate pairing) Assume that E has a twist of degree δ and $m = gcd(k,\delta)$. Let $e = k/m$ and $T_e = T^e \bmod r$, then the reduced twisted Ate pairing is defined as follows :*

$$\begin{array}{rccc} e_{T_e}: & \mathbb{G}_1 \times \mathbb{G}_2 & \to & \mu_r \\ & (P,Q) & \mapsto & f_{T_e,P}(Q)^{\frac{q^k-1}{r}} \end{array}$$

As in the case of Ate pairing, the following theorem ensures that e_{T_e} is a pairing.

Theorem 13. *[40]*

- *$e_T(P,Q)^{LN} = e_{T_e}(P,Q)^{rc}$ where $e_T(P,Q)$ is the Tate pairing, where $c = \sum_{i=0}^{m-1} T^{e(m-1-i)}q^{ei} \equiv mq^{e(m-1)} \bmod r$.*
- *for $r \nmid L$, the twisted Ate pairing e_{T_e} is non-degenerate.*

Remark 15. *The reduced Tate and twisted Ate pairings are defined on $\mathbb{G}_1 \times E(\mathbb{F}_{q^k})$ and $\mathbb{G}_1 \times \mathbb{G}_2$ respectively. So they have the same complexity for each iteration of the Miller algorithm but the*

Miller loop parameter is T^e mod r for the reduced twisted Ate pairing and r for the Tate pairing. Consequently, the twisted Ate pairing will be more efficient than the reduced Tate pairing only for curves with trace t such that T^e mod r is significatively less than r.

Optimal pairings.

The reduction of Miller's loop length is an important way to improve the computation of pairings. The latest work is a generalized method to find the shortest loop when possible, which leads to the concept of optimal pairing [74]. Indeed, observe that if k is the embedding degree with respect to r, then $r|q^k - 1$ but $r \nmid q^i - 1$ for any $1 \leq i < k$. This implies that $r|\Phi_k(q)$ where Φ_k is the $k-th$ cyclotomic polynomial. Since $T \equiv q \bmod r$ where $T = t - 1$, we have $r|\Phi_k(T)$. More generally, if we consider Ate$-i$ pairing, which is a generalisation of Ate pairing with Miller function $f_{T_i,Q}$ where $T_i \equiv q^i \bmod r$, then

$$r|\Phi_{k/g}(T_i), \text{ where } g = gcd(i,k)$$

so that the minimal value for T_i is $r^{1/\varphi(k/g)}$ (where φ is the Euler's totient function) and the lowest bound is $r^{1/\varphi(k)}$, obtained for $g = 1$. We then give the following definition of optimal pairing, this is a pairing that can be computed with the smallest number of iterations in the Miller loop.

Definition 20. *[74] Let $e : G_1 \times G_2 \longrightarrow G_T$ be a non-degenerate, bilinear pairing with $|G_1| = |G_2| = |G_T| = r$, where the field of definition of G_T is $\mathbb{F}_{q^k}$. e is called an optimal pairing if it can be evaluated with about at most $(\log_2 r)/\varphi(k) + \varepsilon(k)$ Miller iterations, where $\varepsilon(k)$ is less than $\log_2 k$.*

The lowest bound is attained for several families of elliptic curves. The following theorem gives the construction of an optimal pairing.

Theorem 14. *[74, Theorem 4] Let E be an elliptic curve defined over $\mathbb{F}_q$. The embedding degree with respect to a large integer r dividing the order of the group $\sharp E(\mathbb{F}_q)$ is denoted k. Let $\lambda = mr$ be a multiple of r such that $r \nmid m$ and write $\lambda = \sum_{i=0}^{l} c_i q^i$. Remember $h_{R,S}$ is the function with divisor $\mathrm{Div}(h_{R,S}) = (R) + (S) - (S+R) - (P_\infty)$ where R and S are two arbitrary points on the elliptic curve E. If $s_i = \sum_{j=i}^{l} c_j q^j$, the map $e_o : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$ defined as*

$$(Q,P) \longmapsto \left(\prod_{i=0}^{l} f_{c_i,Q}^{q^i}(P) \cdot \prod_{i=0}^{l-1} h_{[s_{i+1}]Q,[c_i q^i]Q}(P) \right)^{\frac{q^k-1}{r}}$$

defines a bilinear pairing. Furthermore, the pairing is non degenerate if

$$mkq^k \neq ((q^k-1)/r) \cdot \sum_{i=0}^{l} i c_i q^{i-1} \bmod r.$$

In Section 3.3, we apply the previous theorem to provide an example of optimal pairing on Jacobi quartic curves of embedding degree 8. Observe that the computation of optimal pairings follows the same approach as the computation of the Ate pairing.

3.2 Ate pairing computation on $E_d : Y^2 = dX^4 + Z^4$

In this section, we rewrite formulas for point addition and the Miller function for Ate pairing computation. According to the definition of this pairing, the point addition and point doubling are performed in $\mathbb{F}_{q^k}$. But thanks to the twist we will consider the points $\left(\frac{X_i}{\omega^2} : \frac{Y_i}{\omega^6} : \frac{Z_i}{\omega^3}\right)$ where X_i, Y_i and Z_i belong to $\mathbb{F}_{q^{k/4}}$, $i = 1, 2, 3$. We also know that in Ate pairing the point P is fixed during computations and has its coordinates in the base field $\mathbb{F}_q$. Thus this point can be taken in affine coordinates $(x_P, y_P, 1)$.

3.2.1 Point addition and point doubling on E_d for Ate pairing

In this section, we rewrite formulas for point doubling and points addition on the curve E_d from those in section 2.2.2 of the previous chapter with the difference that the coordinates of points have the form $\left(\frac{X_i}{\omega^2} : \frac{Y_i}{\omega^6} : \frac{Z_i}{\omega^3}\right)$ where X_i, Y_i and Z_i belong to $\mathbb{F}_{q^{k/4}}$, $i = 1, 2, 3$.

Doubling.

$\left(\frac{X_3}{\omega^2} : \frac{Y_3}{\omega^6} : \frac{Z_3}{\omega^3}\right) = 2\left(\frac{X_1}{\omega^2} : \frac{Y_1}{\omega^6} : \frac{Z_1}{\omega^3}\right)$ such that

$$\begin{aligned} X_3 &= 2X_1Y_1Z_1 \\ Z_3 &= Z_1^4 - dX_1^4\omega^4 \\ Y_3 &= 2Y_1^4 - Z_3^2 \end{aligned}$$

Addition.

$\left(\frac{X_3}{\omega^2} : \frac{Y_3}{\omega^6} : \frac{Z_3}{\omega^3}\right) = \left(\frac{X_1}{\omega^2} : \frac{Y_1}{\omega^6} : \frac{Z_1}{\omega^3}\right) + \left(\frac{X_2}{\omega^2} : \frac{Y_2}{\omega^6} : \frac{Z_2}{\omega^3}\right)$ such that

$$\begin{aligned} X_3 &= X_1^2Z_2^2 - Z_1^2X_2^2 \\ Z_3 &= X_1Z_1Y_2 - X_2Z_2Y_1 \\ Y_3 &= (X_1Z_2 - X_2Z_1)^2(Y_1Y_2 + (Z_1Z_2)^2 + d\omega^4(X_1X_2)^2) - Z_3^2 \end{aligned}$$

3.2.2 The Miller function for Ate pairing computation on E_d

The Miller function on the Jacobi quartic $E_d : Y^2 = dX^4 + Z^4$ is given in section 2.2.4 :

$$h_{R,S}(X,Y,Z) = \frac{4X_3^2X^2}{2X_3^2(Y+Z^2) - 2X^2(Y_3+Z_3^2)}\left(\frac{ZY+Z^3}{X^3} - \frac{1}{2}\lambda\left(\frac{Y+Z^2}{X^2}\right) - \frac{\alpha}{4}\right)$$

where

$$\lambda = \begin{cases} \dfrac{-2X_1^3Z_2(Y_2+Z_2^2) + 2X_2^3Z_1(Y_1+Z_1^2)}{X_1X_2[-X_1^2(Y_2+Z_2^2) + X_2^2(Y_1+Z_1^2)]} & \text{if } P_1 \neq P_2 \\ \dfrac{Y_1+2Z_1^2}{X_1Z_1} & \text{if } P_1 = P_2 \end{cases}$$

and

$$\alpha = \begin{cases} \dfrac{-4(Y_1+Z_1^2)(Y_2+Z_2^2)(Z_2X_1 - Z_1X_2)}{X_1X_2[-X_1^2(Y_2+Z_2^2) + X_2^2(Y_1+Z_1^2)]} & \text{if } P_1 \neq P_2 \\ \dfrac{-2Y_1(Y_1+Z_1^2)}{X_1^3Z_1} & \text{if } P_1 = P_2. \end{cases}$$

We follow the notations of section 2.2.5 by setting $-\dfrac{\alpha}{4} = \dfrac{A}{D}$ and $-\dfrac{1}{2}\lambda = \dfrac{B}{D}$. When we replace $(X_i : Y_i : Z_i)$ by $\left(\dfrac{X_i}{\omega^2} : \dfrac{Y_i}{\omega^6} : \dfrac{Z_i}{\omega^3}\right)$ and (X,Y,Z) by $(x_P, y_P, 1)$, a carefully calculation yields to :

$$h_{R,S}(x_P,y_P,1) = \frac{2X_3^2x_P^2}{D\omega^4[X_3^2(y_P+1) - x_P^2(Y_3+Z_3^2)]}\left(B\left(\tfrac{y_P+1}{x_P^2}\right)\omega^3 + A\omega + D\left(\tfrac{(y_P+1)\omega^4}{x_P^3}\right)\right)$$

The factors A, B and D are exactly the same as in the case of Tate pairing but with the main difference that for Ate pairing they are in $\mathbb{F}_{q^{k/4}}$. The addition and doubling formulas for $\left(\dfrac{X_i}{\omega^2} : \dfrac{Y_i}{\omega^6} : \dfrac{Z_i}{\omega^3}\right)$ where X_i, Y_i and Z_i belong to $\mathbb{F}_{q^{k/4}}$, $i = 1,2,3$ clearly show that X_3^2 and $Y_3+Z_3^2$ are also in $\mathbb{F}_{q^{k/4}}$ such that $\dfrac{2X_3^2x_P^2}{D\omega^4[X_3^2(y_P+1) - x_P^2(Y_3+Z_3^2)]} \in \mathbb{F}_{q^{k/4}}$. Then it can be discarded in pairing computation thanks to the final exponentiation. Thus we only have to evaluate

$$h_{R,S}(x_P,y_P,1) = B\left(\frac{y_P+1}{x_P^2}\right)\omega^3 + A\omega + (D\omega^4)\left(\frac{(y_P+1)}{x_P^3}\right)$$

Since $P = (x_P, y_P, 1)$ is fixed during pairing computation, the quantities $\dfrac{(y_P+1)}{x_P^3}$ and $\dfrac{(y_P+1)}{x_P^2}$ can be precomputed once for all steps. Note that each of the multiplications $(D\omega^4)\left(\dfrac{(y_P+1)}{x_P^3}\right)$ and $B\left(\dfrac{y_P+1}{x_P^2}\right)$ costs $\dfrac{k}{4}m_1$.

Remark 16. *We can use the fact that in the expression of $h := h_{R,S}$ the term ω^2 is absent. In this case, in Miller's algorithm, the cost of the main multiplication in $\mathbb{F}_{q^k}$ is not $1m_k$ but $(3/4)m_k$ if we use schoolbook method and is $(8/9)m_k$ if we use Karatsuba multiplication with pairing friendly curves, i.e $k = 2^i3^j$.*

Indeed the main multiplication in Miller's algorithm is of the form $f \cdot h$ where f and h are in

$\mathbb{F}_{q^k}$. *Since* $\mathbb{F}_{q^k}$ *is a* $\mathbb{F}_{q^{k/4}}$*-vector space with basis* $\{1, \omega, \omega^2, \omega^3\}$, f *and* h *can be written as :* $f = f_0 + f_1\omega + f_2\omega^2 + f_3\omega^3$ *and* $h = h_0 + h_1\omega + h_2\omega^2 + h_3\omega^3$ *with* f_i *and* h_i *in* $\mathbb{F}_{q^{k/4}}$, $i = 0, 1, 2, 3$ *and* $h_2 = 0$.

Schoolbook method : *A full multiplication* $f.h$ *in* $\mathbb{F}_{q^k}$ *costs* k^2 *multiplications in the base field* $\mathbb{F}_q$ *using schoolbook method. But thanks to the fact that* $h_2 = 0$, *each of the* 12 *multiplications* $f_i \cdot h_i$ *costs* $\frac{k^2}{16}m_1$, $i = 0, 1, 2, 3$. *Then the total cost of the product* $f \cdot h$ *is* $12\frac{k^2}{16}m_1 = \frac{3k^2}{4}m_1$. *Finally the ratio of the cost in this case by the cost of the general multiplication is* $\frac{\frac{3k^2}{4}}{k^2} = \frac{3}{4}$.

Karatsuba method : *If we are using pairing friendly curves, i.e* $k = 2^i3^j$, *then a full multiplication* $f.h$ *in* $\mathbb{F}_{q^k}$ *costs* 3^i5^j *multiplications in the base field* $\mathbb{F}_q$. *In our case the computation of* $f \cdot h$ *is done by computing, assuming* $h_2 = 0$, *the three products :* $u = (f_0 + f_1\omega)(h_0 + h_1\omega)$ *which costs* $3(3^{i-2}5^j)$, $v = (f_2 + f_3\omega)(h_2 + h_3\omega)$ *which costs* $2(3^{i-2}5^j)$ *and* $w = (f_0 + f_2 + (f_1 + f_3)\omega)(h_0 + h_2 + (h_1 + h_3)\omega)$ *which costs* $3(3^{i-2}5^j)$. *The final cost is then* $8 \cdot 3^{i-2}5^j m_1$ *and the ratio gives* $8/9$.

Remark 17. *Since the coefficients of the Miller function for Ate pairing are the same as for Tate pairing, these coefficients and points operations can be computed in the same manner it was done in the previous chapter with the main difference that computations are done in* $\mathbb{F}_{q^{k/4}}$.

3.2.3 Cost of Ate and Optimal Pairing on E_d

In Table 3.1 and Table 3.2, we summarise and compare the costs for one iteration for both Ate and optimal Ate pairings on the Jacobi curve $E_d : Y^2 = dX^4 + Z^4$ and on the Weierstrass curve $W_d : y^2 = x^3 - 4dx$. We also present these costs in the cases of elliptic curves of embedding degrees 8 and 16.

In Table 3.1 we assume that computations are made in $\mathbb{F}_{q^k}$ using schoolbook method.

Pairings	Doubling		Mixed Addition	
Ate(Q,P) Weierstrass (b=0)[19]	$1m_k + 1s_k + 2m_e + 8s_e + 2em_1 + 1mc$		$1m_k + 9m_e + 5s_e + 2em_1$	
Ate(Q,P) **(This work)**	$3/4m_k + 1s_k + 3m_e + 7s_e + 2em_1 + 1mc$		$3/4m_k + 12m_e + 7s_e + 2em_1 + 1mc$	
Example 1	$k = 8$	$m_1 = s_1 = mc$	$k = 8$	$m_1 = s_1 = mc$
Ate(Q,P) Weierstrass (b=0)[19]	$112m_1 + 24s_1 + 1mc$	$137m_1$	$109m_1 + 10s_1$	$119m_1$
This work	$99m_1 + 22s_1 + 1mc$	$122m_1$	$107m_1 + 14s_1 + 1mc$	$122m_1$
Example 2	$k = 16$	$m_1 = s_1 = m_c$	$k = 16$	$m_1 = s_1 = m_c$
Ate(Q,P) Weierstrass (b=0)[19]	$464m_1 + 48s_1 + 1mc$	$513m_1$	$438m_1 + 20s_1$	$458m_1$
This work	$410m_1 + 44s_1 + 1mc$	$455m_1$	$430m_1 + 28s_1 + 1mc$	$459m_1$

TABLE 3.1 – Comparisons of Ate and optimal Ate pairings formulas on Jacobi quartic and Weierstrass elliptic curves using Schoolbook method

In Table 3.2 we assume that computations are made in $\mathbb{F}_{q^k}$ using Karatsuba method.

Pairings	Doubling		Mixed Addition	
Ate(Q,P) Weierstrass (b=0)[19]	$1m_k + 1s_k + 2m_e + 8s_e + 2em_1 + 1mc$		$1m_k + 9m_e + 5s_e + 2em_1$	
Ate(Q,P) **(This work)**	$8/9m_k + 1s_k + 3m_e + 7s_e + 2em_1 + 1mc$		$8/9m_k + 12m_e + 7s_e + 2em_1 + 1mc$	
Example 1	$k = 8$	$m_1 = s_1 = mc$	$k = 8$	$m_1 = s_1 = mc$
Ate(Q,P) Weierstrass (b=0)[19]	$37m_1 + 51s_1 + 1mc$	$89m_1$	$58m_1 + 15s_1$	$73m_1$
Ate(Q,P) **This work**	$37m_1 + 48s_1 + 1mc$	$85m_1$	$64m_1 + 21s_1 + 1mc$	$86m_1$
Example 2	$k = 16$	$m_1 = s_1 = m_c$	$k = 16$	$m_1 = s_1 = m_c$
Ate(Q,P) Weierstrass (b=0)[19]	$107m_1 + 153s_1 + 1mc$	$261m_1$	$170m_1 + 45s_1$	$215m_1$
Ate(Q,P)**This work**	$107m_1 + 144s_1 + 1mc$	$252m_1$	$188m_1 + 63s_1 + 1mc$	$252m_1$

TABLE 3.2 – Comparisons of Ate and optimal Ate pairings formulas on Jacobi quartic and Weierstrass elliptic curves using Karatsuba method

Remark 18. *If we assume that $m_1 = s_1 = mc$ and Schoolbook multiplication method is used then for Ate pairing computation we obtain in this work a theoretical gain of* 11% *with respect to Weierstrass curves for the doubling step. The improvement is* 4% *when Karatsuba method is used. Our addition step is not better. See Table 3.1 and Table 3.2.*

3.2.4 Comparison

Let us now compare different pairings on Jacobi quartic curves and Weierstrass elliptic curves with quartic twists. Especially we determine the operation counts for the Tate, twisted

Ate, Ate and optimal Ate pairings in a full loop of Miller's algorithm, based on the fastest operations counts summarized in Tables 2.4, 2.5, 3.1 and 3.2. We suppose that we are in the context of optimized pairing such that we can restricted ourselves to the cost of the doubling step. Indeed, in this case r is chosen to have a lower Hamming weight such that the computation in Miller algorithm can be done quickly by skipping many addition steps. For elliptic curves with embedding degrees $k = 8$, we consider the parameters for 112 bits and 128 bits security level. We also consider elliptic curves with embedding degrees $k = 16$ at 128 bits and 192 bits security levels. These values have been selected such that we obtain approximately the same security level both in the elliptic curve defined over the base field $\mathbb{F}_q$ and in the multiplicative group of the finite field $\mathbb{F}_{q^k}$.
For these parameters we give the approximate number of operations in the base field for all the Miller iterations. For the Miller loop in Ate pairing computation we consider an average trace $t \sim \sqrt{q}$. For the values in Table 3.3, we assume that $m_1 = s_1 = mc$. The rows with abbreviation **Kar** means that the values in these rows are obtained using Karatsuba multiplication method whereas the rows started with **Sco** means that the values in these rows are obtained using schoolbook multiplication method. W and J stand for Weierstrass [19] and Jacobi elliptic (this work) curves models respectively, since this work is the first that present the computation of Ate pairing and its variations on Jacobi elliptic curves.

			Tate		twisted Ate		Ate		Optimal Ate	
Parameters	Sec. levels	Arith. in $\mathbb{F}_{q^k}$	W [19]	J (This work)	W [19]	J (This work)	W [19]	J (This work)	W [19]	J (This work)
$k = 8, r \approx 2^{224}$ $q \approx 2^{336}$	112	Kar.	15456	14336	23184	21504	14952	14448	4984	4816
		Sco.	25760	20384	38640	30576	23016	20496	7672	6832
$k = 8, r \approx 2^{256}$ $q \approx 2^{384}$	128	Kar.	17664	16384	26496	24576	17088	16512	5696	5504
		Sco.	29440	23296	44160	34944	26304	23424	8768	7808
$k = 16, r \approx 2^{256}$ $q \approx 2^{320}$	128	Kar.	46336	41472	115840	103680	41760	40320	8352	8064
		Sco.	105216	76544	263040	191360	82080	72800	16416	14560
$k = 16, r \approx 2^{384}$ $q \approx 2^{480}$	192	Kar.	69504	62208	173760	155520	62640	60480	12528	12096
		Sco.	157824	114816	394560	287040	123120	109200	24624	21840

TABLE 3.3 – Comparison of the cost of the various Miller algorithms for pairings on Jacobi quartic curves and Weierstrass curves : $s_1 = m_1 = mc$

From the values in Table 3.3 we draw the following observation : The different pairings computed in this work are always faster in the Jacobi quartic elliptic curves with respect to the Weierstrass elliptic curves. The gain obtained is up to 27% and depends on the method used for multiplications and the security level.

3.3 Implementation and Example

In this section we consider the familly of elliptic curves of embedding degree 8 described in [73] to verify our formulas and to implement the Tate, Ate and optimal Ate pairings. This familly of curves has the following parameters :

$$\begin{aligned} r &= 82x^4 + 108x^3 + 54x^2 + 12x + 1, \\ q &= 379906x^6 + 799008x^5 + 705346x^4 + 333614x^3 + 88945x^2 + 12636x + 745, \\ t &= -82x^3 - 108x^2 - 54x - 8. \end{aligned}$$

For $x = 24000000000010394$, the values of r, q, the trace t and the curve coefficient d are :

$$\begin{aligned} r &= 272056320000471307161600306182614014808404525177076771934828454 76817, \\ q &= 726011672004446604951703464791789328991217313776602768811505320697 581567547878422987036476401963225900 69, \\ d &= 453757295002779128094814665494868330619510821110376730507190825435 988479717424014366897797751227016187 93, \\ t &= -113356800000147285043200063789391713609209096429146 0. \end{aligned}$$

We recall that $\mathbb{G}_1 = E(\mathbb{F}_q)[r]$ and $\mathbb{G}_2 = E\left(\overline{\mathbb{F}_q}\right)[r] \cap \mathrm{Ker}(\pi_q - [q])$. To obtain an optimal pairing in the Jacobi quartic curve E_d with embedding degree 8, we follow the approach described by Vercauteren in [74]. Applying the `ShortestVectors()` function in Magma [12] to the lattice

$$L = \begin{pmatrix} r & 0 & 0 & 0 \\ -q & 1 & 0 & 0 \\ -q^2 & 0 & 1 & 0 \\ -q^3 & 0 & 0 & 1 \end{pmatrix},$$

we obtain the following vector

$$V = [c_0, c_1, c_2, c_3] = [x, 0, 0, 3x + 1].$$

An optimal pairing is then given by :

$$\begin{aligned} e_o : \ \mathbb{G}_2 \times \mathbb{G}_1 &\to \mu_r \\ (Q, P) &\mapsto \left(f_{x,Q}^{3q^3+1}(P) \cdot H_1\right)^{\frac{q^8-1}{r}}, \end{aligned}$$

where $H_1 = (\overline{h}_{[x]Q,[x]Q}(P) \cdot \overline{h}_{[x]Q,[2x]Q}(P) \cdot \overline{h}_{[3x]Q,[1]Q}(P))^{q^3}$ and $s_1 = (3x + 1)q^3$.
Indeed, this is a straightforward application of Theorem 14. From that theorem we have $c_0 =$

$x, c_1 = c_2 = 0, c_3 = 3x + 1$ and $s_i = \sum_{j=i}^{3} c_j q^j$. Observe that for our example $s_1 = s_2 = s_3 = c_3 q^3 = (3x + 1)q^3$. We then apply Theorem 14 to obtain the following

$$e_o(Q, P) = \left(f_{x,Q}(P) \cdot f_{3x+1,Q}^{q^3}(P) \cdot h_{[s_1]Q,[x]Q}(P) \cdot h_{[s_1]Q,P_\infty}^2(P) \right)^{\frac{q^8-1}{r}}.$$

Observe also that $f_{1,Q} = 1$ and $h_{[s_1]Q,P_\infty}^2(P) = 1$. Also, $h_{[s_1]Q,[x]Q}(P)$ will be sent to 1 during the final exponentiation because from $\lambda = mr = \sum_{i=0}^{l} c_i q^i = x + s_1$, we get $[s_1]Q + [x]Q = P_\infty$. We then apply the Property 7 to express $f_{3x+1,Q}$ in terms of $f_{x,Q}$ as follows : $f_{3x+1,Q} = f_{x,Q}^3 \cdot h_{[x]Q,[x]Q} \cdot h_{[x]Q,[2x]Q} \cdot h_{[3x]Q,[1]Q}$. Finally, by using the explanation in Section 3.2, the function $h_{R,S}$ is simplified to $\overline{h}_{R,S}$. We can also observe that, if x is negative then by using the divisors we can take $f_{x,Q} = 1/(f_{-x,Q} \cdot h_{[x]Q,[-x]Q})$ and $h_{[x]Q,[-x]Q}$ is also sent to 1 during the final exponentiation. We remark that for this example, we have $\log_2(x) \approx 54$ iterations of Miller's algorithm which is equal to $\log_2(r)/\varphi(8)$, and this agree with the definition of an optimal pairing.
The Magma code for the implementation of the Tate, Ate and optimal Ate pairings is given in appendix .5 and is also available at
`http://www.prmais.org/Implementation-Pairings-Jacobi.txt`.

Chapitre QUATRE

Arithmetic of a new Edwards model for elliptic curves defined over finite fields

The initial Edwards model for elliptic curves over non-binary fields, with equation $x^2+y^2 = c^2(1+x^2y^2)$ described by Edwards in [28] has been generalised by Bernstein and Lange in [6] to the model defined by the equation $x^2+y^2 = c^2(1+dx^2y^2)$ over non-binary fields. Several models over binary fields (see [7], [8], [79]) have been introduced but without any connection with the initial model. In his thesis, Diao in [23, chapter 7] introduced a new binary Edwards model which is deduced from the well known Edwards model but the addition law is not efficient and not unified.

In this chapter, we present an Edwards model for elliptic curves defined over any finite field and in particular over fields of characteristic 2. This Edwards model is birationally equivalent to the well known Edwards model over non-binary fields. For this, we use theta functions of level 4 to obtain an old model of elliptic curve that we will call a level 4 theta model in this thesis. This model enables us to obtain our new Edwards model with a complete, unified and efficient group law. Over binary fields, we have a competitive formulas for the group law.

The chapter begins in section 4.1 with a brief review of p-adic fields. In section 4.2, we review theta functions and Riemann theta relations of these functions. This enables us to define and give the group law of the level 4 theta model in section 4.3. Section 4.4 focuses on the arithmetic of the Edwards model defined over any finite field. The chapter ends in section 4.5 in which we give efficient and competitive formulas for differential addition on the Kummer line of these curves.

A part of the content of this chapter is a joint work with Oumar Diao which led to the article [24].

4.1 Review on the field of $p-$adic numbers $\mathbb{Q}_p$ and its extensions

This section deals with a brief review of p-adic fields. The results in this section are from [2, Chapter 3]. Another good reference is the book [35].

4.1.1 The field of $p-$adic numbers : $\mathbb{Q}_p$

Definition 21. *Let a be an integer. The $p-$adic valuation of a denoted $v_p(a)$ is the greatest power of p dividing a. By convention $v_p(0) = \infty$. If $r = a/b$ is a rational number its $p-$adic valuation is defined as $v_p(r) = v_p(a) - v_p(b)$*

Definition 22. *Let x be a rational number. The $p-$adic norm is defined as follows :*

$$| x |_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

Building up the $p-$adic field $\mathbb{Q}_p$ from the rational numbers is quite similar to the way to construct the real numbers from $\mathbb{Q}$.

Definition 23. *The set of $p-$adic numbers denoted $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ under the $p-$adic norm.*
The valuation ring of $\mathbb{Q}_p$, the set of $p-$adic integers is $\mathbb{Z}_p = \{x \in \mathbb{Q}_p, | x |_p \leq 1\}$.

$\mathbb{Z}_p$ is an integral domain an its unique maximal ideal is

$$\{x \in \mathbb{Q}_p, | x |_p < 1\} = p\mathbb{Z}_p$$

The residue field of $\mathbb{Q}_p$ is the finite field $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$

Definition 24. *An element $x \in \mathbb{Z}_p$ is called a* lift *of an element $x_0 \in \mathbb{F}_p$ if $\mathcal{P}_1(x) = x_0$, where $\mathcal{P}_1 : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/p\mathbb{Z}_p$ is the canonical projection. In this case, x_0 is the reduction of x.*

This definition can be extended to polynomials with coefficients in $\mathbb{F}_p$ as follows :

Definition 25. *A lift of a polynomial $\overline{P}(x_1, .., x_n) = \overline{a_0} + \overline{a_1}x_1 + ... + \overline{a_n}x_n \in \mathbb{F}_p[x_1, .., x_n]$ is the polynomial $P(x_1, .., x_n) = a_0 + a_1x_1 + ... + a_nx_n \in \mathbb{Z}_p[x_1, .., x_n]$ where a_i is the lift of $\overline{a_i}$; $i = 0, 1, .., n$.*

4.1.2 Finite extension fields of $\mathbb{Q}_p$

Let K be a finite algebraic extension of $\mathbb{Q}_p$. It is always possible to define a norm $|\ .\ |_K$ which extends the $p-$adic norm of $\mathbb{Q}_p$. The valuation ring of K is the integral domain $\mathcal{R} = \{x \in K, |\ x\ |_K \leq 1\}$ with the unique maximal ideal $\mathcal{I} = \{x \in \mathcal{R}, |\ x\ |_K < 1\}$. The residue field of K is the finite field $\mathbb{K} = \mathcal{R}/\mathcal{I}$. It is an algebraic extension of $\mathbb{F}_p$, the residue field of $\mathbb{Q}_p$.

Definition 26. *Let K be a finite algebraic extension of $\mathbb{Q}_p$.*

1. *The* inertia *degree of K denoted f is the degree of the extension $\mathbb{K}$ over $\mathbb{F}_p$.*
2. *The* absolute ramification index *of K is the integer $e = v_K(\psi(p))$ where ψ is the canonical embedding $\mathbb{Z} \longrightarrow \mathbb{Z}_p$ extended to the embedding $\mathbb{Q} \longrightarrow \mathbb{Q}_p$ as follows $\psi(1/x) = 1/\psi(x)$, for all $x \in \mathbb{Z}$ and v_K is a valuation on K.*

The absolute ramification index e and the inertia degree f verify the following relation

Theorem 15. *Let d be the degree of the extension field K over $\mathbb{Q}_p$, then we have $d = ef$.*

Definition 27. *A finite algebraic extension of $\mathbb{Q}_p$ is called* absolutely unramified *if $e = 1$.*

It follows from definition 27 and theorem 15 that for a finite algebraic extension K of degree d of $\mathbb{Q}_p$, there exists an irreducible polynomial $m(x)$ of degree d, lift of an irreducible polynomial over $\mathbb{F}_p$ of degree d, such that the unramified extension of K is $\mathbb{Q}_{p^d} = \mathbb{Z}_{p^d}[x]/(m(x))$.

Definition 28. *The* canonical lift *of an elliptic curve E over a finite field $\mathbb{F}_q$ is an elliptic curve $\mathcal{E}$ over $\mathbb{Q}_q$ which satisfies*

- *The reduction of $\mathcal{E}$ modulo p equals E.*
- *The ring homomorphism $End(\mathcal{E}) \longrightarrow End(E)$ induced by reduction modulo p is an isomorphism.*

Definition 29. *The* Witt vectors *with coefficients in the finite field $\mathbb{F}_q$, $q = p^d$, denoted $W(\mathbb{F}_q)$ is (isomorphic to) the valuation ring of the unramified extension of degree d of $\mathbb{Q}_p$.*

4.2 Theta functions of level 4 in dimension 1

This section is dedicated to the tools that we will use to study our models of elliptic curves in the next sections. All the definitions and results stated in this section can be found in Mumford's Tata lectures in [62]. The thesis of Romain Cossset [17], Damien Robert [67] and Oumar Diao [23] are also good references to understand theta functions. We start with an analogy based on real trigonometric functions to well understand theta functions.

4.2.1 An analogy to understand theta functions

Let t be a real number. We know the following functions :

$$cos(t) = \sum_{n=0}^{+\infty}(-1)^n \frac{t^{2n}}{(2n)!} \text{ and } sin(t) = \sum_{n=0}^{+\infty}(-1)^n \frac{t^{2n+1}}{(2n+1)!}$$

The functions *cos* and *sin* satisfy the algebraic relations :

$$\begin{aligned} cos^2(t) + sin^2(t) &= 1 \\ cos(t_1 + t_2) &= cos(t_1)cos(t_2) - sin(t_1)sin(t_2) \\ sin(t_1 + t_2) &= sin(t_1)cos(t_2) + cos(t_1)sin(t_2) \end{aligned}$$

So, trigonometric functions *cos* and *sin* enable to :

– parametrise the circle : $x^2 + y^2 = 1$

– add two points of this circle as follows : $(x_1, y_1) + (x_2, y_2) = (x_1x_2 - y_1y_2, y_1x_2 + x_1y_2)$

Thus, we will see that as the trigonometric functions defined by series of real functions enable to parametrise a circle, theta functions in dimension 1 which are series of complex functions enable to parametrise elliptic curves and give the addition law on these curves.

4.2.2 Definition and some properties of theta functions in dimension 1

Let $\mathcal{H}_1$ be the upper-half space over $\mathbb{C}$ and $\Omega \in \mathcal{H}_1$. Let $\Lambda_\Omega := \Omega\mathbb{Z} + \mathbb{Z}$ be a lattice of $\mathbb{C}$ and $a, b \in \mathbb{Q}$.

Definition 30. *The Jacobi theta function is the analytic function defined in* $\mathbb{C} \times \mathcal{H}_1$ *by :*

$$\theta(z, \Omega) = \sum_{n\in\mathbb{Z}} \exp\left(\pi i(n^2\Omega + 2nz)\right). \tag{4.1}$$

We now define theta functions with characteristics which are more general.

Definition 31. *The theta function with rational characteristics* (a, b) *is an analytic function defined in* $\mathbb{C} \times \mathcal{H}_1$ *by :*

$$\theta_{a,b}(z, \Omega) = \sum_{n\in\mathbb{Z}} \exp\left(i\pi(n + a)^2\Omega + 2i\pi(n + a)(z + b)\right). \tag{4.2}$$

Remark 19. *The theta function with characteristics generalises the Jacobi theta function because* $\theta_{0,0}(z, \Omega) = \theta(z, \Omega)$

The following proposition gives two important properties of theta functions with characteristics.

Proposition 13. *[62, Pages 121-124] For all $a, b \in \mathbb{Q}$ and for all $m, n \in \mathbb{Z}$, we have :*

$$\theta_{a,b}(z + \Omega m + n, \Omega) = \exp(-i\pi m(m\Omega + 2z)) \exp(2i\pi(an - bm)) \cdot \theta_{a,b}(z, \Omega) \quad (4.3)$$

$$\theta_{a,b}(-z, \Omega) = \theta_{-a,-b}(z, \Omega) = (-1)^{ab}\theta_{a,b}(z, \Omega) \quad (4.4)$$

The property 4.3 means that the theta function with characteristics is $\Lambda_\Omega-$pseudo-periodic. The property 4.4 leads to the following definition.

Definition 32. *The theta function with characteristics, $\theta_{a,b}(z, \Omega)$, is an even function if $(-1)^{ab} = 1$ and is an odd function otherwise.*

Definition 33. *A function $f \in \mathbb{C}$ is $\Lambda_\Omega-$quasi-periodic of level $\ell \in \mathbb{N}^\star$ if for all $z \in \mathbb{C}$ and $m, n \in \mathbb{Z}$, we have : $f(z + \Omega m + n) = \exp(-i\ell\pi m^2\Omega - 2\ell i\pi mz) f(z)$.*

For example it is easy to see that the Jacobi theta function $\theta(., \Omega)$ is quasi-periodic of level 1.

From now on, we are interested by the set of complex functions $\Lambda_\Omega-$ quasi-periodic of level 4 that we should denoted $\mathcal{R}_{4,\Omega}$. All the results that we will state concerning $\mathcal{R}_{4,\Omega}$ are also valuable for $\mathcal{R}_{\ell,\Omega}$ for arbitrary integer $\ell \geq 3$.

Theorem 16. *[62, Section II] The set $\mathcal{R}_{4,\Omega}$ is a $\mathbb{C}-$vector space of dimension 4. Two bases are given by theta functions with characteristics $\mathcal{B}_4 := \left\{\theta_{0,b}(z, 4^{-1}\omega), b \in \frac{1}{4}\mathbb{Z}/\mathbb{Z}\right\}$ and $\mathcal{B}_{(2,2)} := \left\{\theta_{a,b}(2z, \Omega), a, b \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}\right\}$.*

The change of basis between $\mathcal{B}_4$ and $\mathcal{B}_{(2,2)}$ can be obtained by Koizumy formulas stated in the following proposition.

Proposition 14. *[51] The notations are the same as previously stated. The relation between the bases $\mathcal{B}_4$ and $\mathcal{B}_{(2,2)}$ is :*

$$\theta_{0,b}(z, 4^{-1}\Omega) = \sum_{\alpha \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}} \theta_{\alpha,2b}(2z, \Omega). \quad (4.5)$$

Explicitly, it means that if we set $X_{4b}(z) = \theta_{0,b}(z, 4^{-1}\Omega)$ for $b \in \frac{1}{4}\mathbb{Z}/\mathbb{Z}$ and $\theta_{(2i)(2j)}(z) := \theta_{i,j}(2z, \Omega)$ for $i, j \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, then relations between the two bases $\mathcal{B}_4 := \{X_0(z), X_1(z), X_2(z), X_3(z)\}$ and $\mathcal{B}_{(2,2)} := \{\theta_{00}(z), \theta_{01}(z, \Omega/4), \theta_{10}(z), \theta_{11}(z)\}$ are given by the formulas :

$$\begin{cases} X_0(z) = \theta_{00}(z) + \theta_{10}(z) \\ X_1(z) = \theta_{01}(z) + \theta_{11}(z) \\ X_2(z) = \theta_{00}(z) - \theta_{10}(z) \\ X_3(z) = \theta_{01}(z) - \theta_{11}(z) \end{cases} \text{ or } \begin{cases} \theta_{00}(z) = \frac{1}{2}(X_0(z) + X_2(z)) \\ \theta_{01}(z) = \frac{1}{2}(X_1(z) + X_3(z)) \\ \theta_{10}(z) = \frac{1}{2}(X_0(z) - X_2(z)) \\ \theta_{11}(z) = \frac{1}{2}(X_1(z) - X_3(z)) \end{cases} \quad (4.6)$$

These relations will play an important role in the proof of theorem 27.

Remark 20. *According to definition 32, the theta function $z \longmapsto \theta_{\frac{1}{2},\frac{1}{2}}(z)$ is odd and consequently $\theta_{11}(0) = 0$. Therefore, according to the system 4.6 we always have $X_1(0) = X_3(0)$.*

4.2.3 Riemann theta relations

In this section, we recall Riemann theta relations that give algebraic relations between theta functions. These relations will enable us to obtain an elliptic curve that we call the level 4 theta model and the addition law on this elliptic curve. In the following theorem we recall that $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ can be seen as a subgroup of $\mathbb{Z}/4\mathbb{Z}$ via the map $n \longmapsto 4n$. To facilitate notations, we set again $\theta_i(z) := X_i(z) := \theta_{0,i}(z, 4^{-1}\omega)$ for $i \in \mathbb{Z}/4\mathbb{Z}$.

Theorem 21. *[54] Let i, j, k and l be in $\mathbb{Z}/4\mathbb{Z}$ such that $i' = (i+j+k+l)/2, j' = (i+j-k-l)/2, k' = (i-j+k-l)/2$ and $l' = (i-j-k+l)/2$ are in $\mathbb{Z}/4\mathbb{Z}$. Let z_1 and z_2 be elements in $\mathbb{C}$. The theta functions of level four satisfy :*

$$\begin{aligned}&\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} \theta_{i+\eta}(z_1+z_2)\theta_{j+\eta}(z_1-z_2)\theta_{k+\eta}(0)\theta_{l+\eta}(0)\\ &\quad= \sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} \theta_{i'+\eta}(z_1)\theta_{j'+\eta}(z_1)\theta_{k'+\eta}(z_2)\theta_{l'+\eta}(z_2) \qquad (4.7)\end{aligned}$$

Démonstration. : Consider the particular case of [54, Theorem 1] when $g = 1$. If we replace $i+j, i-j, k+l$ and $k-l$ by i, j, k and l, respectively and do the same for i', j', k' and l', then we have

$$\begin{aligned}&\left(\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta)\theta_{i+\eta}(z_1+z_2)\theta_{j+\eta}(z_1-z_2)\right)\left(\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta)\theta_{k+\eta}(0)\theta_{l+\eta}(0)\right)\\ &= \left(\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta)\theta_{i'+\eta}(z_1)\theta_{j'+\eta}(z_1)\right)\left(\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta)\theta_{k'+\eta}(z_2)\theta_{l'+\eta}(z_2)\right) \qquad (4.8)\end{aligned}$$

These Riemann relations (4.8) can be rewritten in the form :

$$\begin{aligned}&\sum_{\eta,\eta'\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta+\eta')\theta_{i+\eta}(z_1+z_2)\theta_{j+\eta}(z_1-z_2)\theta_{k+\eta'}(0)\theta_{l+\eta'}(0)\\ &\quad= \sum_{\eta,\eta'\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} \chi(\eta+\eta')\theta_{i'+\eta}(z_1)\theta_{j'+\eta}(z_1)\theta_{k'+\eta'}(z_2)\theta_{l'+\eta'}(z_2). \qquad (4.9)\end{aligned}$$

Then by summing under all characters χ on the dual $\widehat{\frac{1}{2}\mathbb{Z}/\mathbb{Z}}$, we obtain the desired result. □

Theta functions, or more precisely Riemann relations of theta functions, give a parametrisation of elliptic curves defined over $\mathbb{C}$. It is well known that an elliptic curve over $\mathbb{C}$ is isomorphic to a torus $\mathbb{C}/\Lambda_\omega$. By the classical theory of theta functions, the isomorphism $E \simeq \mathbb{C}/\Lambda_\omega$ gives an embedding into the projective space $\mathbb{P}^3$. For more details, see [63, p. 267]. Moreover, Riemann relations satisfied by theta functions are defined over $\mathbb{C}$. By the Lefschetz principle [70, Section

6], these relations are also valid over any algebraically closed field of characteristic zero. But for characteristic $p > 0$, we consider an elliptic curve E defined by $f(x, y) = 0$ over a finite field $\mathbb{F}_q$ of characteristic p where $q = p^d$ for some positive integer d. We lift the coefficients of $f(x, y)$ to $\mathbb{Z}_q$, the valuation ring of $\mathbb{Q}_q$ which is an unramified extension of $\mathbb{Q}_p$. Let $E_{\mathbb{Z}_q}$ be the canonical lift of E over $\mathbb{Z}_q$ (i.e. $\mathrm{End}(E/\mathbb{F}_q) \simeq_p \mathrm{End}(E/\mathbb{Z}_q)$). We fix an embedding $\mathbb{Q}_q \hookrightarrow \mathbb{C}$ and the Lefschetz principle ensures that algebraic relations defined over $\mathbb{C}$ are also valid over an algebraic extension of $\mathbb{Q}_q$. We then use a reduction modulo p to obtain relations over $\mathbb{F}_q$.

4.3 Level 4 theta model

In this section, we define the level 4 theta model of an elliptic curve, which is valid over any field. We take $z_2 = 0$ in formula (4.7) to obtain two equations that form an elliptic curve over $\mathbb{P}^3(\mathbb{K})$, that we call the level 4 theta model elliptic curve ([61, page 352]) :

$$E'_{\lambda_1,\lambda_2} : \begin{cases} X_0^2 + X_2^2 &= \lambda_1 X_1 X_3 \\ X_1^2 + X_3^2 &= \lambda_2 X_0 X_2 \end{cases}$$

where $X_u = \theta_u(z_1)$, $\lambda_1 = (a_0^2 + a_2^2)/(a_1^2)$ and $\lambda_2 = 2a_1^2/(a_0 a_2)$ with $a_i = X_i(0)$.
The point $[a_0 : a_1 : a_2 : a_3]$ is called the *theta null point*. The numbers $a_i = X_i(0), i = 0, 1, 2, 3$ are called *theta constants* and satisfy the ***Jacobi relation***

$$a_0 a_2 (a_0^2 + a_2^2) = 2a_1^4 \tag{4.10}$$

which implies $\lambda_1 = \lambda_2$. One can consider (see for example [14]) the case where $a_1 = a_3 = 1$ such that the Jacobi relation becomes

$$a_0 a_2 (a_0^2 + a_2^2) = 2. \tag{4.11}$$

The set of points $(a_0, a_2) \in \mathbb{A}^2(\mathbb{K})$ satisfying the relation $a_0 a_2 (a_0^2 + a_2^2) = 2$ is a curve C defined over $\mathbb{K}$. Thus a $\mathbb{K}$-rational point of C defines a level four theta model defined over $\mathbb{K}$. From now on, we present the arithmetic on this curve in the case of finite fields.

4.3.1 Models valid over any finite field

Models over non-binary fields. Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$. Consider $(a_0, a_2) \in \mathbb{A}^2(\mathbb{F}_q)$ such that $a_0 a_2 (a_0^2 + a_2^2) = 2$. Thus in the projective space $\mathbb{P}^3(\mathbb{F}_q)$ with homogeneous coordinates $[X_0 : X_1 : X_2 : X_3]$, the curve given by $E_\lambda : X_0^2 + X_2^2 = \lambda X_1 X_3,\ X_1^2 + X_3^2 = \lambda X_0 X_2$ together with the $\mathbb{F}_q-$ rational point $[a_0 : 1 : a_2 : 1]$ defines an elliptic curve over the finite field $\mathbb{F}_q$.

Models over fields of even characteristic. Let $\mathbb{F}_q$ be a finite field of characteristic 2 and $\mathcal{W}(\mathbb{F}_q)$ the ring of Witt vectors with coefficients in $\mathbb{F}_q$, which is isomorphic to $\mathbb{Z}_q$. So, to obtain the level 4 theta model in even characteristic, it suffices to compute the 2−adic valuation of theta constants. We need the following result from Carls :

Theorem 17. *[14]*
On the canonical lift $E_{\mathcal{W}(\mathbb{F}_q)}$ and for all $i \in \mathbb{Z}/4\mathbb{Z}$, we have

$$a_i^2 = \alpha \sum_{j \in \mathbb{Z}/4\mathbb{Z}} \phi(a_{i+j})\phi(a_j)$$

where ϕ is the lift of the Frobenius of $\mathbb{F}_q$ over $\mathcal{W}(\mathbb{F}_q)$ and $\alpha \in \mathbb{Z}_q$ is a non zero constant.

From this theorem, we have $\alpha(a_0 + a_2) = 1$ and $a_2 = 2\alpha a_0$. Applying the 2-adic valuation, v_2, to both sides of these relations implies that $v_2(a_0) = 0$ and $v_2(a_2) = 1$. Then, there exists $c_0 \in \mathbb{Z}_q$ and $c_2 \in \mathbb{Z}_q$ such that $a_0 = c_0$, $a_2 = 2c_2$ which satisfy the relation $c_0^3 c_2 = 1$. The equations of the level four theta model of elliptic curve over the binary field $\mathbb{F}_q$ is defined as follows :

$$E_\lambda : \begin{cases} X_0^2 + X_2^2 &= \lambda X_1 X_3 \\ X_1^2 + X_3^2 &= \lambda X_0 X_2 \end{cases}, \text{ where } \lambda = c_0^2 \in \mathbb{K}^\star.$$

The identity point is $[c_0 : 1 : 0 : 1]$.

Valid model over any finite field.

Definition 34. *Let $\mathbb{F}_q$ be a finite field. Then a level four theta model is defined by the intersection of two equations :*

$$E_\lambda : \begin{cases} X_0^2 + X_2^2 &= \lambda X_1 X_3 \\ X_1^2 + X_3^2 &= \lambda X_0 X_2 \end{cases}, \text{ where } \lambda = c_0^2 + 4c_2^2$$

The identity point is $[c_0 : 1 : 2c_2 : 1]$.

The coefficients $c_0, c_2 \in \mathbb{F}_q^\star$ satisfy the relation $c_0 c_2 (c_0^2 + 4c_2^2) = 1$. The set of points $(c_0, c_2) \in \mathbb{A}^2(\mathbb{F}_q)$ satisfying this relation is a curve C defined over $\mathbb{F}_q$. The number of rationals points of C is equal to the number of level four theta model defined over $\mathbb{F}_q$. In the above definitions, the condition $\lambda(\lambda^4 - 16) \neq 0$ ensures that the level four theta model E_λ is an elliptic curve. See ([61, page 352]) for details.

It is important to observe that the model that we call level four theta model was introduced in 1966 by Mumford in non-binary fields [61, Page 352]. Over binary fields, Carls [14, section 5.2] obtained the level four theta model but, he did not study the arithmetic of this model. Recently, David Kohel [50] studied the arithmetic of this model that he called a split μ_4-normal form, but only in characteristic 2 and using a different approach than in our case. A comparative study of arithmetic on these curves is done in sections 4.4.4 and 4.5.3.

4.3.2 Addition law on the level 4 theta model

Our addition law comes from Riemann theta relations, which are valid over any finite field.

Theorem 22. *Let $P_1 = [X_0, X_1, X_2, X_3]$ and $P_2 = [Y_0, Y_1, Y_2, Y_3]$ be two points on E_λ defined over a finite field $\mathbb{F}_q$. The coordinates $[Z_0, Z_1, Z_2, Z_3]$ of the point P_3 such that $P_1 + P_2 = P_3$ are given by :*

$$\begin{array}{rcl} Z_0 & = & (X_0^2Y_0^2 + X_2^2Y_2^2) - 4(c_2/c_0)X_1X_3Y_1Y_3 \\ Z_1 & = & a_0(X_0X_1Y_0Y_1 + X_2X_3Y_2Y_3) - 2c_2(X_2X_3Y_0Y_1 + X_0X_1Y_2Y_3) \\ Z_2 & = & (X_1^2Y_1^2 + X_3^2Y_3^2) - 4(c_2/c_0)X_0X_2Y_0Y_2 \\ Z_3 & = & a_0(X_0X_3Y_0Y_3 + X_1X_2Y_1Y_2) - 2c_2(X_0X_3Y_1Y_2 + X_1X_2Y_0Y_3) \end{array} . \quad (4.12)$$

In any finite field, the opposite of the point $P = [X_0 : X_1 : X_2 : X_3]$ is $-P = [X_0 : X_3 : X_2 : X_1]$ (the second coordinate and the fourth coordinate are permuted). The neutral element is $O_0 := [c_0 : 1 : 2c_2 : 1]$.

Démonstration. : Consider $E_\lambda/\mathbb{Z}_q$ the canonical lift of E_λ. Then an equation of $E_\lambda/\mathbb{Z}_q$ is E'_{λ_1,λ_2}. Let $\mathcal{Z}_{i,j} = \theta_i(z_1+z_2)\theta_j(z_1-z_2)$, $\delta_{k,l} = \theta_k(0)\theta_l(0) = a_k a_l$ and
$\mathcal{B}(i',j',k',l') = \sum_{\beta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} \theta_{i'+\beta}(z_1)\theta_{j'+\beta}(z_1)\theta_{l'+\beta}(z_2)\theta_{k'+\beta}(z_2)$,

The equation (4.7) leads to a system of linear equations :

$$(S)\begin{cases} \delta_{k,l}\mathcal{Z}_{i,j} + \delta_{k+2,l+2}\mathcal{Z}_{i+2,j+2} & = & \mathcal{B}(i',j',k',l') \\ \delta_{k+2,l}\mathcal{Z}_{i,j} + \delta_{k,l+2}\mathcal{Z}_{i+2,j+2} & = & \mathcal{B}(i',j',k'+2,l') \end{cases}$$

The determinant of the system (S) is $\det(S) = a_l a_{l+2}(a_k^2 - a_{k+2}^2)$. To avoid a null determinant, we choose $k \notin \{1,3\}$ since $a_1 = a_3$. Cramer's method to solve the system (S) gives :

$$\begin{array}{rcl} \theta_i(z_1+z_2)\theta_j(z_1-z_2) & = & \dfrac{\delta_{k,l+2}\mathcal{B}(i',j',k',l') - \delta_{k+2,l+2}\mathcal{B}(i',j',k'+2,l')}{\delta_{k,l}\delta_{k,l+2} - \delta_{k+2,l+2}\delta_{k+2,l}} \\ & = & \dfrac{a_k\mathcal{B}(i',j',k',l') - a_{k+2}\mathcal{B}(i',j',k'+2,l')}{a_l(a_k^2 - a_{k+2}^2)}. \end{array} \quad (4.13)$$

We fix $k = 0$ and $l = i + j$. Then for $i \in \{0,1,2,3\}$ we factorize (4.13) by $a_0^2 - a_2^2$ in projective coordinates to have :

$$\theta_i(z_1+z_2)\theta_j(z_1-z_2) = \frac{a_0\mathcal{B}(i',j',0,i'+j') - a_2\mathcal{B}(i',j',2,i'+j')}{a_{i+j}}. \quad (4.14)$$

In equation (4.14), if we fix j equal to $0, 1, 2$ and 3, respectively, then we obtain 16 formulas for $i \in \{0,1,2,3\}$ which correspond to four different formulas for addition. Here we consider the case $j = 0$ which gives the addition law formulas in (4.12). We can factorize $\theta_0(z_1 - z_2)$ since we are in projective coordinates. We obtain

$$\theta_i(z_1+z_2)\theta_0(z_1-z_2) = \frac{a_0\mathcal{B}(i',0,0,i') - a_2\mathcal{B}(i',0,2,i')}{a_i} \quad (4.15)$$

For $i \in \{0,1,2,3\}$ and recalling that $c_i = a_i$ if $i \neq 2$, and $2c_2 = a_2$, we have :

$$\begin{aligned}
\theta_0(z_1+z_2)\theta_0(z_1-z_2) &= \frac{c_0\mathcal{B}(0,0,0,0) - 2c_2\mathcal{B}(0,0,2,0)}{c_0},\\
\theta_1(z_1+z_2)\theta_0(z_1-z_2) &= \frac{c_0\mathcal{B}(1,0,0,1) - 2c_2\mathcal{B}(1,0,2,1)}{c_1},\\
\theta_2(z_1+z_2)\theta_0(z_1-z_2) &= \frac{c_0\mathcal{B}(2,0,0,2) - 2c_2\mathcal{B}(2,0,2,2)}{2c_2},\\
\theta_3(z_1+z_2)\theta_0(z_1-z_2) &= \frac{c_0\mathcal{B}(3,0,0,3) - 2c_2\mathcal{B}(3,0,2,3)}{c_3}.
\end{aligned}$$

If $l = i = 2$, the numerator and the denominator of (4.15) can be factorized by 2 before reducing modulo 2. Nevertheless one can avoid a_2 in the denominator by using the alternative relation

$$\theta_i(z_1+z_2)\theta_0(z_1-z_2) = \frac{a_0\mathcal{B}(i',0,0,i'+2) - a_2\mathcal{B}(i',0,2,i'+2)}{a_{i+2}},$$

which gives

$$\theta_2(z_1+z_2)\theta_0(z_1-z_2) = \frac{c_0\mathcal{B}(2,0,0,0) - 2c_2\mathcal{B}(2,0,2,0)}{c_0}.$$

Finally we have :

$$\textcircled{1}\begin{cases}
\theta_0(z_1+z_2)\theta_0(z_1-z_2) = \\
\dfrac{c_0\Big(\theta_0^2(z_1)\theta_0^2(z_2) + \theta_2^2(z_1)\theta_2^2(z_2)\Big) - 4c_2\theta_1(z_1)\theta_3(z_1)\theta_1(z_2)\theta_3(z_2)}{c_0},\\
\theta_1(z_1+z_2)\theta_0(z_1-z_2) = \\
c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_1(z_2) + \theta_2(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)\Big) - \\
2c_2\Big(\theta_2(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2) + \theta_0(z_1)\theta_1(z_1)\theta_2(z_2)\theta_3(z_2)\Big),\\
\theta_2(z_1+z_2)\theta_0(z_1-z_2) = \\
\dfrac{-4c_2\theta_0(z_1)\theta_2(z_1)\theta_0(z_2)\theta_2(z_2) + c_0\Big(\theta_1^2(z_1)\theta_1^2(z_2) + \theta_3^2(z_1)\theta_3^2(z_2)\Big)}{c_0},\\
\theta_3(z_1+z_2)\theta_0(z_1-z_2) = \\
c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_0(z_2)\theta_3(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_1(z_2)\theta_2(z_2)\Big) - \\
2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_3(z_2)\Big)
\end{cases}.$$

We set $Z_i = \theta_i(z_1+z_2), X_i = \theta_i(z_1)$, $Y_i = \theta_i(z_2)$. These relations are valid over $\mathbb{Q}_q$ by the Lefschetz principle. These relations give the theta of the sum $\theta_i(z_1+z_2)$ in terms of $\theta_i(z_1)$ and $\theta_i(z_2)$, and hence the addition formulas in any finite field. □

We present a verification script in the Sage computer algebra system [72] in appendix .7. These formulas are valid modulo any prime p. In characteristic 2, the addition law formulas are

given by :

$$\begin{array}{rcl} Z_0 & = & (X_0Y_0 + X_2Y_2)^2 \\ Z_1 & = & c_0(X_0X_1Y_0Y_1 + X_2X_3Y_2Y_3) \\ Z_2 & = & (X_1Y_1 + X_3Y_3)^2 \\ Z_3 & = & c_0(X_0X_3Y_0Y_3 + X_1X_2Y_1Y_2) \end{array} . \tag{4.16}$$

The neutral element becomes $0_0 := [c_0 : 1 : 0 : 1]$ over binary fields.
The addition laws (4.12) and (4.16) for non-binary and binary fields, respectively, are also valid for doubling : they are unified. More precisely, we can deduce the coordinates $[Z_0 : Z_1 : Z_2 : Z_3] = 2[X_0 : X_1 : X_2 : X_3]$ of the doubling as follows :

$$\left\{ \begin{array}{rcl} Z_0 & = & X_0^4 + X_2^4 - 4(c_2/c_0)X_1^2X_3^2 \\ Z_1 & = & c_0(X_0^2X_1^2 + X_2^2X_3^2) - 4c_2X_0X_1X_2X_3 \\ Z_2 & = & X_1^4 + X_3^4 - 4(c_2/c_0)X_0^2X_2^2 \\ Z_3 & = & c_0(X_0^2X_3^2 + X_1^2X_2^2) - 4c_2X_0X_1X_2X_3 \end{array} \right. \tag{4.17}$$

In binary fields, a reduction modulo 2 yields the following formulas for doubling :

$$\begin{array}{rcl} Z_0 & = & (X_0^2 + X_2^2)^2 \\ Z_1 & = & c_0(X_0^2X_1^2 + X_2^2X_3^2) \\ Z_2 & = & (X_1^2 + X_3^2)^2 \\ Z_3 & = & c_0(X_0^2X_3^2 + X_1^2X_2^2) \end{array} . \tag{4.18}$$

We recall that m_1, s_1 and mc stand for the cost of a multiplication, a squaring and a multiplication by a constant, respectively, in the finite field $\mathbb{F}_q$. In characteristic 2, we have an efficient algorithm to compute point addition formulas (see section 4.4.4 for comparison with previous work). The different costs are given in the following section, where for efficiency, the points are represented as a sextuplet $(X_0 : X_1 : X_2 : X_3 : X_0X_1 : X_2X_3)$. We present a verification script for the formulas in appendix .7.

Cost of the point addition over non-binary fields : $11m_1 + 8s_1 + 6mc$

The sum $(Z_0 : Z_1 : Z_2 : Z_3 : U_3 : V_3)$ of the points represented by $(X_0 : X_1 : X_2 : X_3 : U_1 : V_1)$ and $(Y_0 : Y_1 : Y_2 : Y_3 : U_2 : V_2)$ where $U_1 = X_0X_1$; $V_1 = X_2X_3$ and $U_2 = Y_0Y_1$; $V_2 = Y_2Y_3$ can be computed with the algorithm in Table 4.1.

Cost of point doubling over non-binary fields : $6m_1 + 4s_1 + 3mc$

The algorithm and the cost for computing point doubling are given in Table 4.2.

TABLE 4.1 – Algorithm and cost for point addition.

Operations	*Cost*
$A := X_0Y_0$; $B := X_1Y_1$; $C := X_2Y_2$; $D := X_3Y_3$; $E := A^2$; $F := B^2$;	$4m_1 + 2s_1$
$G := C^2$; $H := D^2$; $Z_0 := E + G + (2c_2/c_0)((B-D)^2 - F - H)$	$3s_1 + 1mc$
$Z_2 := F + H + (2c_2/c_0)((A-C)^2 - E - G)$; $I := 1/2((A+B)^2 - E - F)$	$2s_1 + 1mc$
$J := 1/2((C+D)^2 - G - H)$; $K := (U_1 + V_1)(U_2 + V_2) - I - J$;	$1m_1 + 1s_1$
$L := (A+C)(B+D) - I - J$; $Z_1 := a_0(I+J) - 2c_2K$,	$1m_1 + 2mc$
$E := (X_0 + X_2)(X_3 + X_1) - U_1 - V_1; F := (Y_0 + Y_2)(Y_3 + Y_1) - U_2 - V_2$;	$2m_1$
$G := EF - L$; $Z_3 := c_0L - 2c_2G; U_3 := Z_0Z_1$; $V_3 := Z_2Z_3$	$3m_1 + 2mc$
Total cost : $11m_1 + 8s_1 + 6mc$	

TABLE 4.2 – Algorithm and cost for point doubling in non-binary fields.

Operations	*Cost*
$A := X_0X_2; B := X_1X_3; C := A^2; D := B^2; Z_0 := (\lambda_1^2 - 4c_2^2\lambda_1)D - 2C$;	$2m_1 + 2s_1$
$Z_2 := (\lambda_1^2 - 4c_2^2\lambda_1)C - 2D; E := U_1V_1; F := (U_1 + V_1)^2 - 2E$;	$1m_1 + 1s_1 + 1mc$
$Z_1 := c_0F - 2E; U_3 := Z_0Z_1$;	$1m_1 + 1mc$
$Z3 := c_0(((X_0 + X_1)(X_3 + X_2) - A - B)^2 - 2E) - 4c_2E; V_3 := Z_2Z_3$.	$2m_1 + 1s_1 + 1mc$
Total cost : $6m_1 + 4s_1 + 3mc$	

Cost of the point addition in characteristic 2 : $7m_1 + 2s_1 + 2mc$

We also obtain in a similar manner the following algorithm and costs in the case of binary fields (Table 4.3).

TABLE 4.3 – Algorithm and cost for point addition in binary fields.

Operations	*Cost*
$A := X_0Y_0; B := X_1Y_1; C := X_2Y_2; D := X_3Y_3; Z_0 := (A+C)^2$;	$4m_1 + 1s_1$
$Z_2 := (B+D)^2; Z_1 := c_0(AB + CD); Z_3 := c_0(A+C)(B+D) - Z_1$	$3m_1 + 1s_1 + 2mc$
Total cost : $7m_1 + 2s_1 + 2mc$	

Cost of point doubling in characteristic 2 : $3m_1 + 6s_1 + 2mc$

Table 4.4 present the cost for point doubling in characteristic 2.

TABLE 4.4 – Algorithm and cost for point doubling in binary fields.

Operations	*Cost*
$A := X_0^2; B := X_1^2; C := X_2^2; D := X_3^2; Z_0 := (A+C)^2; Z_2 := (B+D)^2;$	$6s_1$
$Z_1 := c_0(AB + CD); Z_3 := c_0(A+C)(B+D) - Z_1$	$3m_1 + 2mc$
Total cost : $3m_1 + 6s_1 + 2mc$	

4.3.3 Comparison of addition formulas with prior work

In this section, we compare our addition formulas in binary fields with other models of elliptic curves based on currently fastest results found in the Explicit-Formulas Database [5]. We can observe that, in the case where a multiplication by a constant is free, the addition of

TABLE 4.5 – Comparison of points operations in binary fields

Models	Doubling	Addition
Huff [22]	$6m_1 + 5s_1 + 2mc$	$13m_1 + 2s_1 + 2mc$
Weierstrass	$7m_1 + 3s_1$	$14m_1 + 1s_1$
$\mathbb{Z}/4\mathbb{Z}$-normal form [50]	$7m_1 + 2s_1$	$12m_1$
Hessian	$6m_1 + 3s_1$	$12m_1 + 6s_1$
Level 4 theta model	$3m_1 + 6s_1 + 2mc$	$7m_1 + 2s_1 + 2mc$
Binary Edwards [8]	$2m_1 + 5s_1 + 2mc$	$16m_1 + 1s_1 + 4mc$
μ_4-normal form [50]	$2m_1 + 5s_1 + 2mc$	$7m_1 + 2s_1$

points on the level 4 theta model and the μ_4-normal form present the fastest addition formulas among well known models of elliptic curves.

4.3.4 Some properties of the Level Four Theta Model

Lemma 23. *Let E_λ be the level four theta model of an elliptic curve over a finite field $\mathbb{F}_q$. Then E_λ has a rational point of order 4.*

Démonstration. Let $\mathcal{S}_4$ be the group of permutation on $\{0,1,2,3\}$. Let $\sigma = (0,1,2,3)$ be the hull permutation of $\mathcal{S}_4$ and denote by $H_1 = \langle\sigma\rangle$ the subgroup of $\mathcal{S}_4$ generated by σ. Observe that if $P = [X_0 : X_1 : X_2 : X_3]$ is in E_λ, then so are $[X_1 : X_2 : X_3 : X_0], [X_2 : X_3 : X_0 : X_1]$ and $[X_3 : X_0 : X_1 : X_2]$. There exists an action of H_1 on the points of E_λ given by : $\sigma([X_0 : X_1 : X_2 : X_3]) = [X_{\sigma(0)} : X_{\sigma(1)} : X_{\sigma(2)} : X_{\sigma(3)}]$. Under this action, 4 divides the order of E_λ. □

Over non-binary fields, apart from the neutral element $O_0 = [c_0 : 1 : 2c_2 : 1]$, the level 4 theta model has 3 points of order 2 namely : $\widetilde{O}_0 = [-c_0 : 1 : -2c_2 : 1], O_1 := [2c_2 : 1 : c_0 : 1]$ and $\widetilde{O}_1 := [-2c_2 : 1 : -c_0 : 1]$. The four points of order 4 are $A_1 := [1 : 2c_2 : 1 : c_0], \widetilde{A}_1 := [-1 : 2c_2 : -1, c_0], A_2 := [1 : c_0 : 1 : 2c_2]$ and $\widetilde{A}_2 := [-1 : c_0 : -1 : 2c_2]$. Let $P = [X_0 : X_1 : X_2 : X_3]$ be a point on level 4-theta model E_λ, the actions of these rationals points of order 2 and 4 are :

$$\begin{aligned}
P + O_0 &= [X_0 : X_1 : X_2 : X_3], \quad P + \widetilde{O}_0 = [-X_0 : X_1 : -X_2 : X_3], \\
P + O_1 &= [X_2 : X_3 : X_0 : X_1], \quad P + \widetilde{O}_1 = [-X_2 : X_3 : -X_0 : X_1], \\
P + A_1 &= [X_1 : X_2 : X_3 : X_0], \quad P + \widetilde{A}_1 = [-X_1 : X_2 : -X_3 : X_0], \\
P + A_2 &= [X_3 : X_0 : X_1 : X_2], \quad P + \widetilde{A}_2 = [-X_3 : X_0 : -X_1 : X_2].
\end{aligned}$$

These formulas give : $P + \sigma^i(O_0) = \sigma^i(P)$ and $P + \tau^i(O_0) = \tau^i(P)$, from which we can deduce that $\sigma(P) + \sigma(Q) = P + Q + 2\sigma(O_0)$ and $\sigma(P) - \sigma(Q) = P - Q$.

Completeness of group laws. A complete group law means that one can compute the addition of all pairs of input. This property is used to avoid some exceptional procedure attack on elliptic curve cryptosystems [46]. Let E_λ be defined over a non-binary $\mathbb{F}_q$.

Lemma 24. *Let $P = [X_0 : X_1 : X_2 : X_3]$ be a point on E_λ. If $X_i = 0$, then we can write P in the form $\sigma^j([0 : 1 : \pm\sqrt{\pm\varepsilon\lambda} : \pm\varepsilon])$ for some $j \in \{0, 1, 2, 3\}$ where $\varepsilon = \sqrt{-1}$.*

Démonstration. : Without loss of generality, we can assume that $X_0 = 0$. If we have $X_j = 0$ for $j \neq 0$ then according to the equations of the curve, we obtain $P = [0 : 0 : 0 : 0] \notin \mathbb{P}^3$. Therefore $X_j \neq 0$ for $j \neq 0$. Assume also that $X_1 \neq 0$, then $X_2^2 = \lambda X_1 X_3$ and $X_1^2 + X_3^2 = 0$ or equivalently $X_3 = \pm\sqrt{-1}X_1$ and $X_2^2 = \pm\sqrt{-1}\lambda X_1^2$. Then over projective space, we have $P = \sigma^0([0 : 1 : \pm\sqrt{\pm\varepsilon\lambda} : \pm\varepsilon])$. Finally, it means that if $X_i = 0$ and $X_{i+1} \neq 0$ we have $P = \sigma^i([0 : 1 : \pm\sqrt{\pm\varepsilon\lambda} : \pm\varepsilon])$ □

Theorem 25 (Completeness)**.** *The group law on E_λ defined over $\mathbb{F}_q$ is complete if and only if one of the following conditions holds in $\mathbb{F}_q$:*

(1) -1 is not a square in $\mathbb{F}_q$, or

(2) $\sqrt{-1}\lambda$ is not a square in $\mathbb{F}_q$

Démonstration. : For the first part, assume that these conditions do not hold, i.e. $\varepsilon = \sqrt{-1} \in \mathbb{F}_q$ and $\alpha = \sqrt{\varepsilon\lambda_1} \in \mathbb{F}_q$. We will prove that there are two points $P_1, P_2 \in E_\lambda$ such that we can not add P_1 and P_2. Let $P_1 = [0 : 1 : \pm\sqrt{\pm\varepsilon\lambda} : \varepsilon]$ be a point given by lemma 24 and consider the points $P_2 = [\pm c_0\varepsilon : 1 : \pm 2c_2\varepsilon : \pm 1]$. By formulas in equation (4.12), the coordinate Z_2 of $P_1 + P_2$ is equal to zero but $Z_1^2 + Z_3^2$ is not zero, according to the equation of the curve. Hence the group law is not complete. The converse is simple. Indeed, assume that one of the

conditions in the theorem holds. Then it is clear that the coordinates Z_0, Z_1, Z_2 and Z_3 of the sum $P_1 + P_2$ satisfy the equations of the curve. The only point (sum) that must be removed is $[0:0:0:0]$, but according to lemma 24 and by hypothesis, the sum of points can not give this point. So the group law is complete. □

The first sufficient condition of theorem 25 holds when $\mathbb{F}_q$ is of characteristic $p \geq 3$ such that $q \equiv 3 \bmod 4$. Notice that all points of the form $\sigma^i([\pm c_0\varepsilon : 1 : \pm 2c_2\varepsilon : \pm 1])$ given by theorem 25 have an even order, since their coordinates are given by curve constants. This implies that over any finite field (including binary fields), the addition law on the level 4 theta model E_λ is complete in a subgroup of odd order.

4.4 Edwards model for elliptic curves

In [28], Edwards gave a normal form for elliptic curves defined over non-binary fields with an unified addition law. From the level 4 theta model E_λ elliptic curve, we derive an Edwards model which is defined over any finite field and which is birationally equivalent to the Edwards model of [28] over non-binary fields.

4.4.1 Equation of the Edwards model

Theorem 26. *The level 4 theta model E_λ defined over a finite field $\mathbb{F}_q$ is 2-isogenous to an elliptic curve with equation : $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ with the neutral element $O_0 := (2c_2/c_0, 1)$, and $\lambda(\lambda^4 - 16) \neq 0$.*

Démonstration. Consider the map

$$\begin{array}{rccc} \phi : & E_\lambda & \to & \mathcal{E}_\lambda \\ & [X_0 : X_1 : X_2 : X_3] & \longmapsto & (x, y) = (X_2/X_0, X_3/X_1). \end{array}$$

Then we can easily see that

$$1 + x^2 = \lambda \frac{X_1 X_3}{X_0^2} \quad \text{and} \quad y^2 + 1 = \lambda \frac{X_0 X_2}{X_1^2}.$$

Multiply the above two equations to have $(x^2+1)(1+y^2) = \lambda^2 xy$, which can be written as $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$. ϕ maps $[c_0 : 1 : 2c_2 : 1]$ to $O_0 := (2c_2/c_0, 1)$ which becomes $(0, 1)$ over binary fields. □

Theorem 27. *The elliptic curve $\mathcal{E}_\lambda$, with the neutral element $O_0 := (2c_2/c_0, 1)$ defined over a non-binary field is birationally equivalent to the well known Edwards model.*

Démonstration. : Consider the map :

$$\begin{array}{rccc} \varphi : & \mathcal{E}_\lambda & \to & Ec \\ & (x,y) & \longmapsto & \left(\dfrac{x+1}{x-1}, \dfrac{1+y}{1-y}\right) \\ & (2c_2/c_0, 1) & \longmapsto & (0,1) \end{array}$$

φ maps the curve $\mathcal{E}_\lambda$ to the Edwards model $E_c : x^2 + y^2 = c^2(1 + x^2y^2)$, where $c = \dfrac{c_0 - 2c_2}{c_0 + 2c_2}$. The folowing Sage script helps for verification :

```
R.<c0,c2,x,y>=QQ[]
E1=c0*c2*(x^2+y^2+1+x^2*y^2)-(c0^2+4*c2^2)*x*y
S=R.quo([E1])
X=(x+1)/(x-1)
Y=(1+y)/(1-y)
c=(c0-2*c2)/(c0+2*c2)
F=X^2+Y^2-c^2*(1+X^2*Y^2)
S(numerator(F))==0
```

□

Remark 28. *The elliptic curve $\mathcal{E}_\lambda$ enjoys the following property of symmetry like the well known Edwards model of [28] : If the point (x, y) is an element of $\mathcal{E}_\lambda$, then so is (y, x).*

According to remark 28, Theorems 26 and 27, we have this definition :

Definition 35. *An Edwards model for elliptic curves defined over a finite field $\mathbb{F}_q$ is given by the equation :*

$$\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy.$$

with the neutral element $O_0 := (2c_2/c_0, 1)$ and where $\lambda = c_0^2 + 4c_2^2$ satisfies $\lambda(\lambda^4 - 16) \neq 0$

Theorem 29. *The Edwards model $\mathcal{E}_\lambda$ defined over $\mathbb{F}_q$ is non-singular if $\lambda(\lambda^4 - 16) \neq 0$.*

Démonstration. : This follows immediately from the condition for non sigularity of the level 4 theta model. □

Apart from the neutral element $O_0 := (2c_2/c_0, 1)$, the Edwards model $\mathcal{E}_\lambda : 1+x^2+y^2+x^2y^2 = \lambda xy$ has three $2-$torsion rationals points : $P_2 = (1/\gamma, 1), P_3 = (-\gamma, -1)$ and $P_4 = (-1/\gamma, -1)$, where $\gamma = 2c_2/c_0$. The Edwards model $\mathcal{E}_\lambda$ also has four 4-torsion points which are rationals over

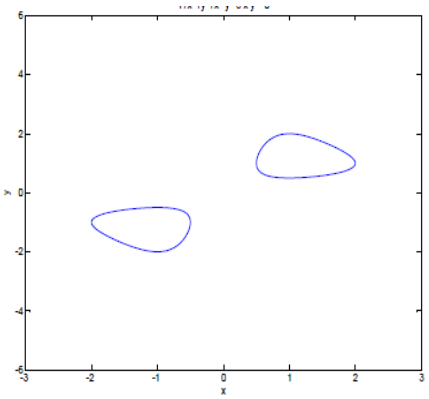

FIGURE 4.1 – The Edwards curve $1 + x^2 + y^2 + x^2y^2 = 5xy$ over $\mathbb{R}$.

$\mathbb{F}_q : Q_1 = (1, \gamma), Q_2 = (1, 1/\gamma), Q_3 = (-1, -\gamma)$ and $Q_4 = (-1, -1/\gamma)$. The actions of rationals points of order 2 and 4 are :

$$\begin{array}{ll} (x,y) + O = (x,y), & (x,y) + P_2 = (1/x, 1/y) \\ (x,y) + P_3 = (-x,-y), & (x,y) + P_4 = (-1/x, -1/y) \\ (x,y) + Q_1 = (1/y, x), & (x,y) + Q_2 = (y, 1/x) \\ (x,y) + Q_3 = (-1/y, -x), & (x,y) + Q_4 = (-y, -1/x) \end{array},$$

Remark 30. If $\mathbb{F}_q$ is a binary field, then $P_3 = O$, $P_4 = P_2$, $Q_3 = Q_1$ and $Q_4 = Q_2$. The number of rationals points of $\mathcal{E}_\lambda$ is then divisible by 4.

4.4.2 Birational equivalence with Weierstrass models

Theorem 31. *Let $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ be the Edwards model of elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic $p \geq 0$.*

(1) if $p \neq 2$, then $\mathcal{E}_\lambda$ is birationally equivalent to a cubic Weierstrass model;

(2) if $p = 2$, then $\mathcal{E}_\lambda$ is birationally equivalent to the Weierstrass model $v^2 + uv = u^3 + 1/\lambda^4$.

Démonstration. : Theorem 27 gives the birational equivalence between $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ and the well known Edwards model $X^2 + Y^2 = c^2(1 + X^2Y^2)$. This well known Edwards model is birationally equivalent to the quartic $Z^2 = c^2X^4 - (c^4 + 1)X^2 + c^2$. Setting $X = 2c(u - c^4 - 1)/v$ and $Z = -c + uX^2/(2c)$, the quartic $Z^2 = c^2X^4 - (c^4 + 1)X^2 + c^2$ is birationally equivalent to the cubic Weierstrass model $v^2 = u^3 - (1 + c^4)u^2 - 4c^4u + 4c^4(1 + c^4)$. This proves (1).

For fields of characteristic 2, the birational map and its inverse between Edwards model and

Weierstrass model are

$$\begin{aligned}(u,v) &\longmapsto (x,y)=\left(\frac{1}{\lambda u},\frac{\lambda^2 v+1}{\lambda^2 u+\lambda^2 v+1}\right) \text{ and } (0,1)\mapsto[0:1:0]\\ (x,y) &\longmapsto (u,v)=\left(\frac{1}{\lambda x},\frac{\lambda y+x(y+1)}{\lambda^2 x(y+1)}\right) \text{ and } [0:1:0]\mapsto(0,1).\end{aligned}$$

which ends the proof (see also [23, p. 65]). □

Corollary 32 ($j-$Invariant)**.** *The $j-$Invariant of the Edwards model $\mathcal{E}_\lambda$ defined over a finite field $\mathbb{F}_q$ is*

$$j=\frac{((c_0^4-4c_0^3c_2+8c_0^2c_2^2+16c_0c_2^3+16c_2^4)(c_0^4+4c_0^3c_2+8c_0^2c_2^2-16c_0c_2^3+16c_2^4))^3}{(c_2c_0(c_0-2c_2)(c_0+2c_2)(c_0^2+4c_2^2))^4}.$$

if $\mathbb{F}_q$ is a non-binary field and the $j-$Invariant is $j=\lambda^4$ if $\mathbb{F}_q$ is a binary field.

Démonstration. Suppose that $\mathbb{F}_q$ is a non-binary field. The $j-$Invariant of the Weierstrass model $v^2=u^3-(1+c^4)u^2-4c^4u+4c^4(1+c^4)$ over $\mathbb{F}_q$ is :

$$j_W=2^4\frac{((c^4-2c^3+2c^2+2c+1)(c^4+2c^3+2c^2-2c+1))^3}{(c(c-1)(c+1)(c^2+1))^4}.$$

Since $c=(c_0-2c_2)/(c_0+2c_2)$, a straightforward calculation gives the desired result. Notice that the expression of j is defined modulo any prime p, then j is defined over fields of any characteristic. Over fields of characteristic 2, we have $j \bmod 2=(c_0/c_2)^4=\lambda^4$ which is the $j-$Invariant of Weierstrass model $v^2+uv=u^3+1/\lambda^4$ in theorem 31. □

4.4.3 Addition on the Edwards model

In [23], Diao uses addition formulas on the known Edwards model [28] to deduce an addition on his binary Edwards model. Over binary fields, the addition law in [23, Theorem 7.4] is not unified and not efficient. However, to have an unified and more efficient addition law formulas we use the addition law on the level 4 theta model. More precisely we have :

Theorem 33. *Let (x_1,y_1) and (x_2,y_2) be two points of $\mathcal{E}_\lambda$. The coordinates of the sum $(x_3,y_3)=(x_1,y_1)+(x_2,y_2)$ are given by :*

$$(x_3,y_3)=\left(\frac{c_0(x_1+y_1x_2y_2)-2c_2(y_1+x_1x_2y_2)}{c_0(y_2+x_1y_1x_2)-2c_2(x_2+x_1y_1y_2)},\frac{c_0(x_1x_2+y_1y_2)-2c_2(x_1y_2+y_1x_2)}{c_0(1+x_1y_1x_2y_2)-2c_2(x_1y_1+x_2y_2)}\right). \quad (4.19)$$

The opposite of the point is $-(x_1,y_1)=(x_1,1/y_1)$ and the neutral element is $O_0:=(2c_2/c_0,1)$.

One can verify the addition law on new Edwards model $\mathcal{E}_\lambda$ by this sage script [72] :

```
R.<c0,c2,x1,y1,x2,y2> = QQ[]
E1 = c0*c2*(x1^2 + y1^2 + 1 + x1^2*y1^2) -
     (c0^2 + 4*c2^2)*x1*y1
E2 = c0*c2*(x2^2 + y2^2 + 1 + x2^2*y2^2) -
     (c0^2 + 4*c2^2)*x2*y2
S = R.quo([E1,E2])
Nx3 = c0*(x1 + y1*x2*y2) - 2*c2*(y1 + x1*x2*y2)
Dx3 = c0*(y2 + x1*y1*x2) - 2*c2*(x2 + x1*y1*y2)
Ny3 = c0*(x1*x2 + y1*y2) - 2*c2*(x1*y2 + y1*x2)
Dy3 = c0*(1 + x1*x2*y1*y2) - 2*c2*(x1*y1 + x2*y2)
x3 = Nx3/Dx3; y3 = Ny3/Dy3

E3 = c0*c2*(x3^2 + y3^2 + 1 + x3^2*y3^2) -
     (c0^2 + 4*c2^2)*x3*y3
S(numerator(E3)) == 0
```

Over fields of characteristic 2, the coordinates of the sum of two points are obtained by a reduction modulo 2 :

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 + y_1 x_2 y_2}{y_2 + x_1 y_1 x_2}, \frac{x_1 x_2 + y_1 y_2}{1 + x_1 y_1 x_2 y_2} \right). \tag{4.20}$$

Remark 34. *Addition group law is unified over any fields, i.e. addition formulas are also valid for point doubling. The point doubling formulas can be written as follows :*

$$2(x_1, y_1) = \left(\frac{c_0 x_1 (1 + y_1^2) - 2c_2 y_1 (1 + x_1^2)}{c_0 y_1 (1 + x_1^2) - 2c_2 x_1 (1 + y_1^2)}, \frac{c_0 (x_1^2 + y_1^2) - 4c_2 x_1 y_1}{c_0 (1 + x_1^2 y_1^2) - 4c_2 x_1 y_1} \right). \tag{4.21}$$

Over binary fields, the formulas (4.20) or (4.21) give the doubling formulas :

$$2(x_1, y_1) = \left(\frac{x_1 (1 + y_1)^2}{y_1 (1 + x_1)^2}, \frac{(x_1 + y_1)^2}{(1 + x_1 y_1)^2} \right). \tag{4.22}$$

According to theorems 25 and 26, the addition law on Edwards model $\mathcal{E}_\lambda$ is complete over any subgroup of $\mathcal{E}_\lambda$ of odd order.

Explicit formulas

Affine coordinates. Let (x_1, y_1) and (x_2, y_2) be two points on the Edwards model $\mathcal{E}_\lambda$: $1 + x^2 + y^2 + x^2 y^2 = \lambda^2 xy$ defined the field $\mathbb{F}_q$. The following formulas compute the sum

$(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$, when it is defined :

$$\begin{aligned}
&A = x_1 \cdot y_1; B = x_2 \cdot y_2; C = x_1 + y_1 \cdot B; D = y_1 + x_1 \cdot B; E = y_2 + x_2 \cdot A;\\
&F = x_2 + y_2 \cdot A; G = A + B; H = (x_1 + y_2) \cdot (x_2 + y_1) - G;\\
&I = (x_1 + y_1) \cdot (x_2 + y_2) - H; J = 1 + A \cdot B; x_3 = (c_0 \cdot C - 2c_2 \cdot D)/(c_0 \cdot E - 2c_2 \cdot F);\\
&y_3 = (c_0 \cdot H - 2c_2 \cdot I)/(c_0 \cdot J - 2c_2 \cdot G)
\end{aligned}$$

These formulas cost $2I+9m_1+8mc$ over non-binary fields and $2I+5m_1$ over binary fields, where I is the costs of a field inversion. Remark that, the opposite of a point costs 1 inversion which is too expensive. Nevertheless the sum and the difference of two points (x_1, y_1) and (x_2, y_2) have the same complexity. Indeed, the following formula computes the difference $(x_4, y_4) = (x_1, y_1) - (x_2, y_2)$, if it is defined :

$$\begin{aligned}
&(x_4, y_4) =\\
&\left(\frac{c_0(x_1y_2 + y_1x_2) - 2c_2(x_1x_2 + y_1y_2)}{c_0(1 + x_1y_1x_2y_2) - 2c_2(x_1y_1 + x_2y_2)}, \frac{c_0(y_1 + x_1x_2y_2) - 2c_2(x_1 + y_1x_2y_2)}{c_0(y_2 + x_1y_1x_2) - 2c_2(x_2 + x_1y_1y_2)}\right).
\end{aligned} \tag{4.23}$$

We retrieve the eight polynomials used to compute the sum : $F_1 = x_1 + y_1x_2y_2, F_2 = y_1 + x_1x_2y_2, F_3 = y_2 + x_1y_1x_2, F_4 = x_2 + x_1y_1y_2, F_5 = x_1x_2 + y_1y_2, F_6 = x_1y_2 + y_1x_2, F_7 = 1 + x_1y_1x_2y_2$ and $F_8 = x_1y_1 + x_2y_2$. Therefore formulas (4.19) and (4.23) can be rewritten as follows :

$$\begin{aligned}
(x_1, y_1) + (x_2, y_2) &= \left(\frac{c_0F_1 - 2c_2F_2}{c_0F_3 - 2c_2F_4}, \frac{c_0F_5 - 2c_2F_6}{c_0F_7 - 2c_2F_8}\right),\\
(x_1, y_1) - (x_2, y_2) &= \left(\frac{c_0F_6 - 2c_2F_5}{c_0F_7 - 2c_2F_8}, \frac{c_0F_2 - 2c_2F_1}{c_0F_3 - 2c_2F_4}\right).
\end{aligned}$$

Projective coordinates. In this paragraph, we embeds the curve $\mathcal{E}_\lambda$ in $\mathbb{P}^2$ by setting the new coordinate $t = xy$. For efficiency reason in the computation of the sum and doubling of points, We follow the approach of Hisil et al. in [43] by using the extended projective coordinates $[X : Y : Z : T]$ in $\mathbb{P}^3$ where $x = X/Z, y = Y/Z, t = T/Z, T = XY/Z$ and $Z \neq 0$. The projective closure of the curve in $\mathbb{P}^3$ is then $Z^2 + X^2 + Y^2 + T^2 = \lambda^2 TZ$.

Addition of points.

The coordinates of the sum $[X_3 : Y_3 : Z_3 : T_3] = [X_1 : Y_1 : Z_1 : T_1] + [X_2 : Y_2 : Z_2 : T_2]$ are :

$$\begin{aligned}
X_3 &= (X_1Z_2 + Y_1T_2)(Z_1Z_2 + T_1T_2)\\
Y_3 &= (X_1X_2 + Y_1Y_2)(Z_1Y_2 + X_2T_1)\\
Z_3 &= (Z_1Z_2 + T_1T_2)(Z_1Y_2 + X_2T_1)\\
T_3 &= (X_1Z_2 + Y_1T_2)(X_1X_2 + Y_1Y_2)
\end{aligned}$$

The computation of X_3 costs $5m_1$:X_1Z_2, Y_1T_2, Z_1Z_2 and T_1T_2. The same argument follows for Y_3. This enables the cost of Z_3 and T_3 to be $1m_1$ each, since their factors are already computed in X_3 and Y_3. The total cost of the addition of two points is $12m_1$

Doubling of a point.

The coordinates of the doubling $[X_3 : Y_3 : Z_3 : T_3] = 2[X_1 : Y_1 : Z_1 : T_1]$ are :

$$\begin{aligned} X_3 &= (X_1Z_1 + Y_1T_1)(Z_1 + T_1)^2 \\ Y_3 &= (Y_1Z_1 + X_1T_1)(X_1 + Y_1)^2 \\ Z_3 &= (Y_1Z_1 + X_1T_1)(Z_1 + T_1)^2 \\ T_3 &= (X_1Z_1 + Y_1T_1)(X_1 + Y_1)^2 \end{aligned}$$

The computation of X_3 costs $3m_1 + 1s_1$:$X_1Z_1, T_1Y_1, (X_1 + Y_1)^2$ and the main product. The same argument follows for Y_3. This enables the cost of Z_3 and T_3 to be $1m_1$ each, since their factors are already computed in X_3 and Y_3. The total cost of the doubling is $8m_1 + 2s_1$.

4.4.4 Comparison of addition formulas on level 4 theta model and Edwards models with other models

In this section, we compare our addition formulas in binary fields with other models of elliptic curves based on the fastest results of Explicit-Formulas Database [5]. Recall that m_1, s_1 and mc are the cost of multiplication, square and multiplication by a constant, respectively, over a finite field. We can observe that, in the case where a multiplication by a constant is free,

TABLE 4.6 – Comparison of points operations in binary fields

Models	Doubling	Addition
Huff of [22]	$6m_1 + 5s_1 + 2mc$	$13m_1 + 2s_1 + 2mc$
Weierstrass	$7m_1 + 3s_1$	$14m_1 + 1s_1$
Our Edwards model	$8m_1 + 2s_1$	$12m_1$
$\mathbb{Z}/4\mathbb{Z}$-normal form [50]	$7m_1 + 2s_1$	$12m_1$
Hessian	$6m_1 + 3s_1$	$12m_1 + 6s_1$
Level 4 theta model	$3m_1 + 6s_1 + 2mc$	$7m_1 + 2s_1 + 2mc$
Binary Edwards	$2m_1 + 5s_1 + 2mc$	$16m_1 + 1s_1 + 4mc$
μ_4-normal form [50]	$2m_1 + 5s_1 + 2mc$	$7m_1 + 2s_1$

the addition of points on the level 4 theta model and the μ_4-normal form present the fastest

addition formulas among well known models of elliptic curves. This also means that the level 4 theta model offers good performances in scalar multiplication algorithms that perform many additions : For example the Montgomery's ladder, addition chain method and fixed base point methods such as Yao's method and Euclidean method. see [2, Chapter 13] for more details about these algorithms.

4.5 Differential addition on Kummer line

We recall that the Kummer line $\mathcal{K}_E$ of an elliptic curve E is the singular projective curve obtained by quotienting E by the inverse automorphism acting on it. In other words, the Kummer line is simply the set of coordinates invariant under taking inverses. An immediate consequence is that the group law on E does not induce a group law on the Kummer line, since we cannot distinguish a point and its opposite. But given two points P and Q, one can compute $P+Q$ if $P-Q$ is known. This kind of operation is called a pseudo addition or differential addition. It has many important applications in cryptography : efficient representation of points, computation of the exponentiation, pairing computation with theta functions. In the next sections, we will compute differential addition on both the level 4 theta model and our Edwards model of elliptic curves.

4.5.1 Differential addition on the level 4 theta model

This section is devoted to the differential addition on Kummer line of elliptic curves. Let $\mathbb{F}_q$ be a finite field and let E_λ be the level 4 theta model of ordinary elliptic curve defined over $\mathbb{F}_q$. Let $P = [X_0 : X_1 : X_2 : X_3]$ be a point on E_λ, the opposite of P is $[X_0 : X_3 : X_2 : X_1]$. The set $\{X_0, X_2, X_1 + X_3\}$ is invariant under the action of opposite. Denote $W_1 = X_1 + X_3$, then an equation of Kummer line in non-binary fields is

$$\mathcal{K}_{E_\lambda} : W_1^2 = \frac{2}{\lambda}(X_0^2 + X_2^2) + \lambda X_0 X_2,$$

and is

$$W_1^2 = \lambda X_0 X_2$$

over binary fields. The addition on E_λ does not induce an addition law on the corresponding Kummer line, since we can not distinguish a point and its opposite, but one can define a differential addition on Kummer line. Let $P = [X_0 : X_1 : X_2 : X_3]$ and $Q = [Y_0 : Y_1 : Y_2 : Y_3]$ be two points on E_λ and let $P + Q = [Z_0 : Z_1 : Z_2 : Z_3], P - Q = [T_0 : T_1 : T_2 : T_3]$ and $2P = [U_0 : U_1 : U_2 : U_3]$. For differential addition and differential doubling we express

the coordinates Z_0, Z_2 and U_0, U_2 in terms of the coordinates of X_0, X_2, T_0, T_2 and X_0, X_2, respectively. We have :

$$\begin{cases} Z_0 &= (X_0^2Y_0^2 + X_2^2Y_2^2) - 4(c_2/c_0)X_1X_3Y_1Y_3 \\ Z_1 &= c_0(X_0X_1Y_0Y_1 + X_2X_3Y_2Y_3) - 2c_2(X_2X_3Y_0Y_1 + X_0X_1Y_2Y_3) \\ Z_2 &= (X_1^2Y_1^2 + X_3^2Y_3^2) - 4(c_2/c_0)X_0X_2Y_0Y_2 \\ Z_3 &= c_0(X_0X_3Y_0Y_3 + X_1X_2Y_1Y_2) - 2c_2(X_0X_3Y_1Y_2 + X_1X_2Y_0Y_3) \end{cases}$$

$$\begin{cases} T_0 &= (X_0^2Y_0^2 + X_2^2Y_2^2) - 4(c_2/c_0)X_1X_3Y_1Y_3 \\ T_1 &= c_0(X_0X_1Y_0Y_3 + X_2X_3Y_2Y_1) - 2c_2(X_2X_3Y_0Y_3 + X_0X_1Y_2Y_1) \\ T_2 &= (X_1^2Y_3^2 + X_3^2Y_1^2) - 4(c_2/c_0)X_0X_2Y_0Y_2 \\ T_3 &= c_0(X_0X_3Y_0Y_1 + X_1X_2Y_3Y_2) - 2c_2(X_0X_3Y_3Y_2 + X_1X_2Y_0Y_1) \end{cases}$$

$$\begin{cases} U_0 &= X_0^4 + X_2^4 - 4(c_2/c_0)X_1^2X_3^2 \\ U_1 &= c_0(X_0^2X_1^2 + X_2^2X_3^2) - 4c_2X_0X_1X_2X_3 \\ U_2 &= X_1^4 + X_3^4 - 4(c_2/c_0)X_0^2X_2^2 \\ U_3 &= c_0(X_0^2X_3^2 + X_1^2X_2^2) - 4c_2X_0X_1X_2X_3 \end{cases}$$

A straightforward and easy calculation, while considering the equations of the curve, give the following formulas.

We present a verification script in the Sage computer algebra system [72] in appendix .8.

$$\begin{cases} Z_0 &= T_0 \\ Z_2 &= \frac{c_0^2-4c_2^2}{c_0c_2}X_0Y_0 \cdot X_2Y_2 - T_2 \end{cases}, \tag{4.24}$$

$$\begin{cases} U_0 &= (1-4c_0c_2^3)(X_0^2+X_2^2)^2 - 2X_0^2X_2^2 \\ U_2 &= \frac{1-4c_0c_2^3}{c0^2c2^2}X_0^2 \cdot X_2^2 - 2c_0^2c_2^2(X_0^2+X_2^2)^2 \end{cases}, \tag{4.25}$$

The cost of differential addition is $3m_1 + 1mc$: Indeed, the points $P = [X_0 : X_1 : X_2 : X_3]$, $Q = [Y_0 : Y_1 : Y_2 : Y_3]$ and $P - Q = [T_0 : T_1 : T_2 : T_3]$ are known. So the computation of Z_0 is free and Z_2 requires the computations of the three products $A = X_0 \cdot Y_0, B = X_2 \cdot Y_2, C = A \cdot B$ and the following multiplication by a constant $\frac{c_0^2-4c_2^2}{c_0c_2} \cdot C$. Following the same approach, the cost of the differential doubling for computing U_0 and U_2 is $1m_1 + 3s_1 + 3mc$. Indeed we need the three squarings $A = X_0^2, B = X_2^2, C = (A+B)^2$, only one multiplication $D = A \cdot B$ and the three multiplications by constants $(1-4c_0c_2^3) \cdot C$, $\frac{1-4c_0c_2^3}{c0^2c2^2} \cdot D$ and $(2c_0^2c_2^2) \cdot C$.

Over binary fields, formulas (4.24) and (4.25) are

$$\begin{cases} Z_0 &= T_0 \\ Z_2 &= \frac{c_0}{c_2}X_0Y_0 \cdot X_2Y_2 + T_2 \end{cases}, \tag{4.26}$$

$$\begin{cases} U_0 &= (X_0^2+X_2^2)^2 \\ U_2 &= \frac{1}{c0^2c2^2}X_0^2 \cdot X_2^2 \end{cases}, \tag{4.27}$$

The differential addition in binary fields cost $3m_1 + 1mc$: Indeed we use the same procedure explained earlier in the case of non-binary fields. Thus we have the three multilpications $A = X_0 \cdot Y_0, B = X_2 \cdot Y_2$, $C = A \cdot B$ and the multiplication with a constant $\frac{c_0}{c_2} \cdot C$.
Similarly the cost of the differential doubling is $1M+3S+1m$, which consists of the computation of $A = X_0^2, B = X_2^2, C = (A+B)^2$, $D = A \cdot B$ and the multiplication by a constant $\frac{1}{c0^2 c2^2} X_0^2 \cdot D$. Notice that, moreover, we can also focus on the computation of the coordinate functions W_i for $i = 3, 5$, which give the addition law on the Kummer line $\mathcal{K}_{E_\lambda} : W^2 = \frac{2}{\lambda}(X_0^2 + X_2^2) + \lambda X_0 X_2,$. Finally we have :

$$\begin{aligned} W_3 &= W_1 \cdot W_2 \cdot \Big(c_0(X_0 \cdot Y_0 + X_2 \cdot Y_2) - 2c_2(X_0 Y_2 + X_2 Y_0) \Big) - W_4 \\ W_5 &= \frac{c_0}{c_0^2 + 4c_2^2}(c_0^2 - 4c_2^2)(X_0^2 + X_2^2) \cdot (W_1^2 - 2c_0 c_2 (X_0^2 + X_2^2)) \end{aligned}$$

where $W_1 = X_1 + X_3, W_2 = Y_1 + Y_3, W_3 = Z_1 + Z_3, W_4 = T_1 + T_3$ and $W_5 = U_1 + U_3$.
The computations cost $6m_1 + 3mc$ and $2m_1 + 4s_1 + 5mc$ operations for differential addition and doubling, respectively, over non-binary fields. Over binary fields, these costs are $5m_1 + 2mc$ and $2m_1 + 4s_1 + 2mc$ for differential addition and doubling, respectively.

4.5.2 Differential addition on the Edwards model over any finite field

Let $\mathcal{E}_\lambda$ be the Edwards model and let (x, y) be a point on $\mathcal{E}_\lambda$. The first coordinate of a point (x, y) on $\mathcal{E}_\lambda$ is invariant under the negation action. We Consider the points (x_i, y_i) on $\mathcal{E}_\lambda$ for $i = 1, 2, 3, 4$ such that $(x_3, y_3) = (x_1, y_1) + (x_2, y_2), (x_4, y_4) = (x_1, y_1) - (x_2, y_2)$ and $(x_5, y_5) = 2(x_1, y_1)$. As in section 4.5.1, our goal is to express x_3 in term of x_1, x_2, x_4 and x_5 in terms of x_1. We recall that $x_1 = X_2/X_0, y_1 = X_3/X_1$, $x_2 = Y_2/Y_0, y_2 = Y_3/Y_1$, $x_3 = Z_2/Z_0, y_3 = Z_3/Z_1$, $x_4 = T_2/T_0, y_4 = T_3/T_1$ and $x_5 = U_2/U_0, y_5 = U_3/U_1$ A direct computation from formulas (4.24) and (4.25) give, if they are defined :

$$x_3 + x_4 = \frac{(c_0^2 - 4c_2^2)x_1 x_2}{c_0 c_2[1 + x_1^2 x_2^2 - 4c_0 c_2^3(1 + x_1^2 + x_2^2 + x_1^2 x_2^2)]}, \tag{4.28}$$

$$x_5 = \frac{(1 - 4c_0 c_2^3)x_1^2 - 2c_0^4 c_2^4 (1 + x_1^2)^2}{c_0^2 c_2^2[(1 - 4c_0 c2^3)(1 + x_1^2)^2 - 2x_1^2]}. \tag{4.29}$$

To avoid inversions in affine coordinates, let $x_i = X_i/Z_i$ for $i = 1, 2, 3, 4, 5$ where $[X : Z]$ parametrizes the projective space $\mathbb{P}^1$. Over any finite fields, formulas (4.28) and (4.29) become :

$$\begin{cases} X_3 = (c_0^2 - 4c_2^2)X_1 X_2 Z_1 Z_2 Z_4 - X_4 B \\ Z_3 = Z_4 B \end{cases} \tag{4.30}$$

where $B = Z_1^2Z_2^2 + X_1^2X_2^2 - 4c_0c_2^3(Z_1^2Z_2^2 + X_1^2Z_2^2 + X2^2Z_1^2 + X_1^2X_2^2)$

$$\begin{cases} X_5 &= (1-4c_0c_2^3)X_1^2Z_1^2 - 2c_0^4c_2^4(Z_1^2+X_1^2)^2 \\ Z_5 &= c_0^2c_2^2[(1-4c_0c_2^3)(Z_1^2+X_1^2)^2 - 2X_1^2Z_1^2] \end{cases} . \tag{4.31}$$

The computation of $[X_3 : Z_3]$ costs $8m_1 + 4s_1 + 1mc : Z_1Z_2, X_1Z_2, X2Z_1, X_1X_2$, their squares and the two products $X_1X_2 \cdot Z_1Z_2 \cdot Z_4$. The computational cost of the differential addition can be reduced to $6m_1 + 4s_1 + 1c$ if $Z_4 = 1$. The computation of $[X_5 : Z_5]$ costs $1m_1 + 2s_1 + 3mc$: $X_1Z_1, (X_1+Z_1)^2 - 2x_1Z_1, (X_1Z_1)^2$.
Similarly, over fields of characteristic 2, formulas (4.28) and (4.29) become :

$$\begin{cases} X_3 &= c_0X_1X_2Z_1Z_2Z_4 \\ Z_3 &= Z_4Z_1^2Z_2^2 + X_1^2X_2^2 \end{cases} , \tag{4.32}$$

$$\begin{cases} X_5 &= X_1^2Z_1^2 \\ Z_5 &= c_0^2c_2^2(Z_1+X_1)^4) \end{cases} . \tag{4.33}$$

The formula (4.32) costs $6m_1 + 2s_1 + 1mc : Z_1Z_2, X_1X_2$, their squares and the two products $X_1X_2 \cdot Z_1Z_2 \cdot Z_4$. If $Z_4 = 1$ then the formula (4.32) can be computed with $4m_1 + 2s_1 + 1mc$. The formula (4.33) costs $1m_1 + 3s_1 + 1mc : X_1Z_1, (X_1+Z_1)^2, ((X_1+Z_1)^2)^2$.
Formulas (4.32) correspond to Stam [71] formulas and formulas (4.33) correspond to Gaudry and Lubicz formulas [34].

4.5.3 Comparison with previous work on differential addition

Over non-binary fields, Brier and Joye [13] generalize the idea of Montgomery [60] on general Weierstrass model $v^2 = u^3 + b_2u + b_6$. The method of [13] uses $6m_1 + 2s_1 + 2mc$ per bits for a scalar multiplication, i.e. multiply a point on Kummer line by a scalar. The best known formula (see table 4.7) uses $3m_1 + 6s_1 + 3mc$ per bits and is due to Gaudry and Lubicz in [34] on Kummer model of Legendre form $v^2 = u(u-1)(u-b)$. Our formula costs $4m_1 + 3s_1 + 4mc$ on the level 4 theta model. So, over non-binary fields, if we assume in the worse case that $s_1 = m_1 = mc$ then our formula for the level four theta model and those of Gaudry and Lubicz [34] are the best formulas to date for differential addition.

Over binary fields, the best known formula (see table 4.8) due to Kohel [50], costs $4m_1 + 4s_1 + 2mc$. Our formula requires $4m_1 + 3s_1 + 2mc$ on the level 4 theta model and is slightly faster than the Kohel's split μ_4-normal form [50]. The formulas on the level 4 theta model are the best to compute on Kummer line over binary fields.

TABLE 4.7 – Comparisons of differential addition over non-binary fields

model	differential doubling	differential addition	Total
Montgomery [60]	$2m_1 + 2s_1 + 1mc$	$3m_1 + 2s_1$	$5m_1 + 4s_1 + 1mc$
Weierstrass	$4m_1 + 3s_1 + 2mc$	$6m_1 + 2s_1 + 2mc$	$10m_1 + 5s_1 + 4mc$
Our Edwards model	$1m_1 + 2s_1 + 3mc$	$6m_1 + 4s_1 + 1mc$	$7m_1 + 6s_1 + 4mc$
Gaudry and Lubicz [34]	$4s_1 + 2mc$	$2m_1 + 2s_1 + 1mc$	$2m_1 + 6s_1 + 3mc$
Level 4 theta model	$1m_1 + 3s_1 + 3mc$	$3m_1 + 1mc$	$\mathbf{4m_1 + 3s_1 + 4mc}$

TABLE 4.8 – Comparisons of differential addition over binary fields

model	differential doubling	differential addition	Total
Weierstrass of [71]	$1m_1 + 3s_1 + 1mc$	$4m_1 + 1s_1$	$5m_1 + 4s_1 + 1mc$
Binary Edwards of [8]	$1m_1 + 3s_1 + 1mc$	$4m_1 + 1s_1 + 1mc$	$5m_1 + 4s_1 + 2mc$
Huff of [22]	$1m_1 + 3s_1 + 1mc$	$4m_1 + 2s_1$	$5m_1 + 5s_1 + 1mc$
Edwards model of [79]	$1m_1 + 4s_1 + 1mc$	$4m_1 + 2s_1$	$5m_1 + 6s_1 + 1mc$
Gaudry and Lubicz [34]	$1m_1 + 3s_1 + 1mc$	$3m_1 + 2s_1$	$4m_1 + 5s_1 + 1mc$
μ_4-normal form [50]			$4m_1 + 4s_1 + 2mc$
Level 4 theta model	$1m_1 + 3s_1 + 1mc$	$3m_1 + 1mc$	$\mathbf{4m_1 + 3s_1 + 2mc}$

Conclusion

In this thesis, we used the geometric intersection of the group law to obtain efficient and competitive formulas in the doubling and addition steps in Miller's algorithm for Tate pairing computation on Jacobi intersection elliptic curves. We use a different approach, namely an isomorphism between Weierstrass model of elliptic curves and the special Jacobi quartic elliptic curve $Y^2 = dX^4 + Z^4$ to obtain the Miller function associated to this quartic to compute the Tate pairing, Ate pairing and its variations on this curve. Our results on this curve appear to be the most efficient among curves with quartic twists. We finally use the theory of theta functions to obtain a new Edwards model of elliptic curve which is defined over any finite field. An intermediate model, called level 4 theta model, is used. We study the arithmetic of these curves. We show that the group law, obtained by the Riemann relations of theta functions, is complete and unified. In particular, the addition in characteristic 2 and the differential addition on the Kummer lines of theses curves are competitive.
At the end of this work, some questions remain open and can directed us for future work :

1. Investigate pairings computation on our new Edwards model of elliptic curves and the level 4 theta model using Miller's algorithm.
2. Complete the computation of pairings in characteristic 2 on elliptic curves using theta functions.
3. Investigate Elliptic Curve Method factorization based on our new Edwards model of elliptic curves.
4. Find a set of complete addition group law on the new models.

Bibliographie

[1] Arene, C., Lange, T., Naehrig, M. et Ritzenthaler, C. *Faster computation of the Tate pairing.* Dans : *Journal of number theory* vol. 131(5), pp. 842-857 (2011).

[2] Avanzi, R. et al. *Handbook of Elliptic and Hyperelliptic curve Cryptography.* Dans : *Discrete Math. Aplli. Chapman and Hall* (2006).

[3] Balasubramanian, R. et Koblitz, N. *The improbability that an elliptic curve has sub-exponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm.* Dans : *Journal of Cryptology* vol. 11 , pp. 141-145 (1998).

[4] Barreto, P. S. L. M., Galbraith, S.D, OhEigeartaigh, C. et Scott, M. *Efficient pairing computation on supersingular abelian varieties.* Dans : *Designs, Codes and Cryptography* vol. 42(3), pp. 239-271 (2007).

[5] Bernstein, D. et Lange, T. *Explicit-formulae database.* Dans : *http://www.hyperelliptic.org/EFD* ().

[6] Bernstein, D. et Lange, T. *Faster Addition and Doubling on Elliptic Curves.* Dans : *ASIACRYPT 2007, Springer Berlin / Heidelberg.* vol. 4833 , pp. 29-50 (2007).

[7] Bernstein, D. J., Birkner, P., Joye, M., Lange, T. et C., Peters. *Twisted Edwards curves.* Dans : *AFRICACRYPT 2008, LNCS, Springer,* vol. 5023, pp. 389-405, (2008).

[8] Bernstein, D.J., Lange, T. et Farashahi, R.R. *Binary Edwards curves.* Dans : *CHES 2008, LNCS, Springer,* Vol. 5154 , pp. 244-265, (2008).

[9] Billet, O. et Joye, M. *The Jacobi model of an elliptic curve and side-channel analysis.* Dans : *AAECC 2003, LNCS* vol. 2643, pp. 34-42 (2003).

[10] Blake, I.F., Seroussi, G. et Smart, N.P. *Advances in Elliptic Curves in Cryptography.* Dans : *London Mathematic Society, Cambridge University Press* (2005).

[11] Boneh, D. et Franklin, M. *Identity based encryption from the Weil pairing.* Dans : *LNCS* vol. 2139 , pp. 213-229 (2001).

[12] Bosma W., Cannon J. et Playout, C. *The Magma algebra system I. The user language.* Dans : *J. Symbolic Comput.* vol. 24(3-4), pp. 235-265 (1997).

[13] Brier, E. et Joye, M. *Weierstrass elliptic curves and side-channel attacks.* Dans : *Public Key Cryptography, LNCS, Springer* vol. 2274, pp. 335-345, (2002).

[14] Carls, R. *Theta null points of 2-adic canonical lifts.* Dans : *A preprint is available at* `http://arxiv.org/math.NT/0509092` (2005).

[15] Chudnovsky, D. V et Chudnovky, G. V. *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* dans : *Advances in Applied Mathematics* vol. 7(4), pp. 385-434 (1986).

[16] Cocks, C. *An identity based encryption scheme based on quadratic residues.* Dans : *Cryptography and Coding, LNCS* vol. 2260 , pp.360-363 (2001).

[17] Cosset, R. *Application des fonctions thêta à la cryptographie sur les courbes hyperelliptiques.* Dans : *Université Henri Poincaré - Nancy 1-France* (2011).

[18] Costello, C., Hisil, H., Boyd, C., Nieto, J.M.G. et Wong, K.K.H. *Faster pairings on special Weierstrass curves.* Dans : *Pairing 2009, LNCS* vol. 5671, pp. 89-101 (2009).

[19] Costello, C., Lange, T. et Naehrig, M. *Faster pairing computations on curves with high-degree twists.* Dans : *PKC 2010, LNCS* vol. 6056, pp. 224-242 (2010).

[20] D. Boneh, B. Lynn et Shacham, H. *Short signatures from the Weil pairing.* Dans : *Technical report 2003:* `http://crypto.stanford.edu/~dabo/abstracts/weilsigs.html`. vol. , pp. (2003).

[21] Das, M.P.L. et Sarkar, P. *Pairing computation on twisted Edwards form elliptic curves.* Dans : *Pairing 2008, LNCS* vol. 5209, pp. 192-210 (2008).

[22] Devigne, J. et Joye, M. *Binary Huff curves.* Dans : *Topics in Cryptology – CT-RSA 2011, vol. 6558 of LNCS pp. 340-355, Springer* (2011).

[23] Diao, 0. *Quelques aspects de l'arithmétique des courbes hyperelliptique de genre 2.* Dans : *Université de Rennes 1 - France* (2010).

[24] Diao, O. et Fouotsa, E. *Arithmetic of the Level Four Theta Model of Elliptic Curves.* Dans : *Afrika Mathematica. (DOI) 10.1007/s13370-013-0203-1 (Springer)* vol. , pp. (2013).

[25] Duquesne, S, El Mrabet, N. et Fouotsa, E. *Efficient pairing computation on Jacobi quartic elliptic curve.* Dans : *Submitted. :* vol., pp. (2012).

[26] Duquesne, S. et Fouotsa, E. *Tate Pairing computation on Jacobi's elliptic curves.* Dans : *Pairing-Based Cryptography, Pairings 2012, LNCS Springer verlag.* vol. 7708, pp. 254-269 (2012).

[27] Dutta, R., Barua, R. et Sarkar, P. *Pairing-based cryptography : A survey.* Dans : *Cryptology ePrint Archive* Report 2004/064 (2004).

[28] Edwards, H. M. *A normal form for elliptic curves.* Dans : *Bulletin of the AMS 44(2007), pp. 393-422, URL: http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html* (2007).

[29] Feng, R., Nie, M. et Wu, H.S. *Twisted Jacobi Intersections Curves.* Dans : *Theory and applications of models of computations, LNCS* vol. 6108, pp. 199-210 (2010).

[30] Freeman, D., M., Scott et Teske, E. *A taxonomy of pairing-friendly elliptic curves.* Dans : *Journal of cryptology* vol. 23(2), pp. 224-280 (2010).

[31] Frey, G., Muller, M. et Ruck, H. *The Tate Pairing and the Discrete Logarithm applied to Elliptic Curve Cryptosystems.* Dans : *IEEE Transactions on Information Theory* vol. 45(5), pp. 1717-1719 (1999).

[32] Galbraith, S.D. *Pairings.* Dans : *London Mathematics Society Lecture Note Series - Cambridge University Press* vol. 317, pp. 183-213 (2005).

[33] Galbraith, S.D., McKee, J.F. et Valenca, P.C. *Ordinary abelian varieties having small embedding degree.* Dans : *Finite Fields Applications* vol. 13, pp. 800-814 (2007).

[34] Gaudry, P. et Lubicz., D. *The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines.* Dans : *Finite Fields and Their Applications* (2009).

[35] Gouvêa, F.Q. *P-adic Numbers, An introduction.* Dans : *Springer-Verlag, 2nd edition* (1997).

[36] Goyal, V., Pandey, O., Sahai, A. et Waters., B. *Attribute-based encryption for fine-grained access control of encrypted data.* Dans : *Proceedings of the 13th ACM conference on Computer and communications security* vol. , pp. 98-98 (2006).

[37] Gu, H., Gu, D. et Xie, Wenlu. *Efficient Pairing Computation on Elliptic Curves in Hessian Form.* Dans : *ICISC 2010, LNCS* vol. 6829, pp. 169-176 (2011).

[38] Hankerson, D., Menezes, A. et Vanstone, S. *Guide to elliptic curve cryptography.* Dans : *Springer-Verlag* (2004).

[39] Hartshorne, R. *Algebraic curves.* Dans : *Springer-Verlag, Graduate Texts in Mathematics* vol. 52 (1977).

[40] Hesse, F., Smart, N.P. et Vercauteren, F. *The Eta Pairing Revisited.* Dans : *IEEE Transactions on Information Theory* vol. 52(10), pp. 4595-4602 (2006).

[41] Hisil, H., K.K., Wong, Carter, G. et Dawson, E. *Faster Group Operations on Elliptic Curves.* Dans : *Australasian Information Security Conference(AISC),Wellington, New Zealand* vol. 98, pp. 7-19 (2009).

[42] Hisil, H., K.K., Wong, Carter, G. et Dawson, E. *Jacobi Quartic Curves revisited.* Dans : *ACISP 2009, LNCS, Springer* vol. 5594, pp. 452-468 (2009).

[43] Hisil, H., K.K., Wong, Carter, G. et Dawson, E. *Twisted Edwards Curves revisited.* Dans : *ASIACRYPT 2008, LNCS, Springer* vol. 5350, pp. 326-343 (2008).

[44] Hoffstein, J., Pipher, J. et Silvermann, J.H. *An Introduction to Mathematical Cryptography.* Dans : *Undergraduate texts in Mathematic, Springer* (2008).

[45] Ionica, S. et Joux, A. *Another approach to pairing computation in Edwards coordinates.* Dans : *INDOCRYPT 2008, LNCS* vol. 5365, pp. 400-413 (2008).

[46] Izu, T. et Takagi, T. *Exceptional procedure attack on elliptic curve cryptosystems.* Dans : *PKC 2003 , LNCS, Springer* vol. 2567, pp. 224-239 (2003).

[47] Joux, A. *A one-round protocol for tripartite Diffie-Hellman.* Dans : *In Algorithmic Number Theory Symposium- ANTS IV, LNCS* vol. 1838, pp. 385-394 (2000).

[48] Koblitz, N. *Elliptic Curves cryptosystems.* Dans : *Mathematics of computation* vol. 48 pp. 203-209 (1987).

[49] Koblitz, N. et Menezes, A. *Pairing-based cryptography at high security levels.* Dans : *Cryptography and Coding, LNCS* vol. 3796, pp. 13-36 (2005).

[50] Kohel, D. *Efficient arithmetic on elliptic curves in characteristic 2.* Dans : *INDOCRYPT 2012, LNCS Springer* vol.7668 , pp.378-398 (2012).

[51] Koizumi, S. *Theta relations and projective normality of abelian varieties.* Dans : *American Journal of Mathematics, pp: 865-889* (1976).

[52] Libert, B. et Quisquater, J.-J. *Identity based undeniable signatures.* Dans : *Topics in Cryptology – CT-RSA 2004, LNCS* vol. 2964 , pp. 112-125 (2004).

[53] Lichtenbaum, S. *Duality theorems for curves over p-adic fields.* Dans : *Inventiones Math.* vol. 7 pp. 120-136 (1969).

[54] Lubicz, D. et Robert, D. *Efficient Pairing Computation With Theta Functions.* Dans : *preprint available at* `http://perso.univ-rennes1.fr/david.lubicz/articles/pairing.pdf` (2010).

[55] Menezes, A., Okamoto, T. et Vanstone, S.. *Reducing elliptic curve logarithms to logarithms in a Finite Field.* Dans : *IEEE Transactions on Information Theory* vol. 39(5), pp. 1639-1646 (1993).

[56] Merriman, J.R., Siksek, S. et Smart, N.P. *Explicit 4-descents on an elliptic curve.* Dans : *Acta Arithmetica* vol. 77, pp. 385-404 (1996).

[57] MILLER, V. *A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of groups.* Dans : *Mathematics of computation* vol. 62 pp. 865-874 (1994).

[58] MILLER, V. *Short programs for functions on curves.* Dans : *Unpublished manuscript available at* `http://crypto.stanford.edu/miller/miller.pdf.` vol. (1986).

[59] MILLER, V. *Use of elliptic curves in cryptography.* Dans : *LNCS* vol. 218 pp. 417-426 (1986).

[60] MONTGOMERY, P.L. *Speeding up the Pollard and elliptic curve methods of factorization.* Dans : *Mathematics of Computation 48(177) pp:243-264* (1987).

[61] MUMFORD, D. *On the equations defining abelian varieties I.* Dans : *Invent. Math., pp. 287–354* (1966).

[62] MUMFORD, D. *Tata lectures on theta I.* Dans : *Birkhäuser Boston Inc., Boston, MA* (1983).

[63] MUMFORD, D. *The red book of varieties and schemes.* Springer-verlag, 2004.

[64] NIST. *National Institute of Standards and Technology.* Dans : *available at* `http://csrc.nist.gov/publications/PubsSPs.html` vol. 800-57 (2007).

[65] POLLARD, J. *Monte Carlo Methods for Index Computation mod p.* Dans : *Mathematics of Computation* vol. 32 pp. 918-924 (1978).

[66] RIVEST, S., SHAMIR, A. et ADLEMAN. *A method for obtaining digital signatures and public-key cryptosystems.* Dans : *Communications of the ACM* vol. 21(2) , pp. 120-126 (1978).

[67] ROBERT, D. *Fonctions thêta et applications à la cryptographie.* Dans : *PhD 1 thesis – Université Henri Poincaré – Nancy 1* (2010).

[68] SAKAI, R., OHGISHI, K. et KASAHARA, M. *Cryptosystems based on pairing.* Dans : *Symposium on Cryptography and Information Security* vol. , pp. (2000).

[69] SHAMIR, A. *Identity based cryptosystems and signature schemes.* Dans : *CRYPTO 1984, LNCS* vol. 196, pp. 47-53 (1985).

[70] SILVERMANN, J.H. *The Arithmetic of elliptic curves.* Dans : *Graduate texts in Mathematics, Springer-Verlag* vol. 106 (1986).

[71] STAM, M. *On Montgomery-like representations for elliptic curves over $GF(2^k)$.* Dans : *PKC 2003 pp. 240-254* (2002).

[72] Stein, W. *Sage Mathematics Software (Version 4.8).* Dans : *The Sage Group* (2012). `http://www.sagemath.org`.

[73] Tanaka, S. et Nakamula, K. *More constructing pairing-friendly elliptic curves for cryptography.* Dans : vol. , pp. (2007).

[74] Vercauteren, F. *Optimal pairings.* Dans : *IEEE Transactions on Information Theory* vol. 56(1), pp. 455-461 (2010).

[75] Verheul, E.R. *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems.* Dans : *EUROCRYPT 2001. Springer-Verlag, LNCS* vol. 2045 , pp. 195-210 (2001).

[76] Wang, H., Wang, K., Zhang, L. et Li, Bao. *Pairing Computation on Elliptic Curves of Jacobi Quartic Form.* Dans : *Chinese Journal of electronics* vol. 20(4), pp. 655-661 (2011).

[77] Washington, L.C. *Elliptic Curves, Number Theory and Cryptography.* Dans : *Discrete Math .Aplli, Chapman and Hall* (2008).

[78] Weil, A. *Courbes algébriques et variétés abéliennes.* Dans : *Hermann* vol. (1948).

[79] Wu, H., Tang, C. et Feng, R. *A New Model of Binary Elliptic Curves with Fast Arithmetic.* Dans : *Cryptology ePrint Archive, Report 2010/608* (2010). `http://eprint.iacr.org/`.

[80] Zhang, L., Wang, K., Wang, H. et Ye, D. *Another Elliptic curves model for faster pairing computation.* Dans : *ISPEC, LNCS* vol. 6672, pp. 432-446 (2011).

Liste des tableaux

Appendix

.1 Addition law formulas on Jacobi Intersection curves

```
//////////Formulas for point addition on Jacobi Intersection///////
R.<a, X1, Y1, X2, Y2, Z1, Z2, T1, T2> = QQ[]

E11 = X1^2+Y1^2- T1^2

E12 = a*X1^2+Z1^2-T1^2

E21 = X2^2+Y2^2- T2^2

E22 = a*X2^2+Z2^2-T2^2

S=R.quo([E11, E12, E21, E22])

X3=X1*T1*Y2*Z2 + Y1*Z1*X2*T2

Y3=Y1*T1*Y2*T2 - X1*Z1*X2*Z2

Z3=Z1*T1*Z2*T2 - a*X1*Y1*X2*Y2

T3=T1^2*Y2^2 + Z1^2*X2^2

E31 = X3^2+Y3^2- T3^2

E32 = a*X3^2+Z3^2-T3^2
S(E31)==0
```

```
S(E32)==0

////////////////////Formulas for point doubling on Jacobi intersection/////
R.<a, X1, Y1, Z1, T1> = QQ[]

E11 = X1^2+Y1^2- T1^2

E12 = a*X1^2+Z1^2-T1^2

S=R.quo([E11, E12])
X3=2*X1*T1*Y1*Z1

Y3=-Z1^2*T1^2 - a*X1^2*Y1^2  + 2*( X1^2*Y1^2 + Y1^4)

Z3=Z1^2*T1^2 - a*X1^2*Y1^2

T3=Z1^2*T1^2  + a*X1^2*Y1^2

E31 = X3^2+Y3^2- T3^2

E32 = a*X3^2+Z3^2-T3^2

S(E31)==0

S(E32)==0

////////////////Algorithm to compute point Addition on Jacobi Intersection/////////////
R.<a, X1, Y1, X2, Y2, Z1, Z2, T1, T2> = QQ[]

E11 = X1^2+Y1^2- T1^2

E12 = a*X1^2+Z1^2-T1^2

E21 = X2^2+Y2^2- T2^2
```

```
E22 = a*X2^2+Z2^2-T2^2

S=R.quo([E11, E12, E21, E22])

U1=X1*Y1; V1=Z1*T1

U2=X2*Y2; V2=Z2*T2
E=X1*Z2; F=Y1*T2; G=Z1*X2;  H=T1*Y2; J=U1*V2; K=V1*U2

X3=(H+F)*(E+G)-J-K;

Y3= (H+E)*(F-G)-J+K

Z3=(V1-a*U1)*(U2+V2)+a*J-K

T3=(H+G)^2-2*K

U3=X3*Y3; V3=Z3*T3

E31 = X3^2+Y3^2- T3^2

E32 = a*X3^2+Z3^2-T3^2

S(E31)==0

S(E32)==0

///Algorithm to compute point doubling on Jacobi intersection   ///////
R.<a, X1, Y1, Z1, T1> = QQ[]

E11 = X1^2+Y1^2- T1^2

E12 = a*X1^2+Z1^2-T1^2

S=R.quo([E11, E12])
```

```
U1=X1*Y1; V1=Z1*T1

E=V1^2; F=U1^2; G=a*F;

T3=E+G

Z3=E-G

Y3=2*(F+Y1^4)-T3

X3=(U1+V1)^2-E-F

U3=X3*Y3; V3=Z3*T3
E31 = X3^2+Y3^2- T3^2

E32 = a*X3^2+Z3^2-T3^2

S(E31)==0

S(E32)==0
```

.2 Addition law formulas on Jacobi quartic curves

```
 ////////////////////  Formulas for point Addition on Jacobi quartic ////////////////

R.<d, X1, Y1, X2, Y2, Z1, Z2> = QQ[]

E1= Y1^2-d*X1^4- Z1^4

E2 = Y2^2-d*X2^4- Z2^4
S=R.quo([E1, E2])
X3=X1^2*Z2^2- Z1^2*X2^2
Z3=X1*Z1*Y2 - X2*Z2*Y1
Y3=(X1*Z2-X2*Z1)^2 *(Y1*Y2 + (Z1*Z2)^2 + d*(X1*X2)^2)- Z3^2
E3 = Y3^2 - d*X3^4 - Z3^4
```

```
S(E3)==0
//////////////Formulas for point doubling on Jacobi quartic//////
R.<d, X1, Y1, Z1> = QQ[]
E1= Y1^2-d*X1^4- Z1^4
S=R.quo([E1])
X3=2*X1*Y1*Z1
Z3=Z1^4 - d*X1^4
Y3=2*Y1^4 -Z3^2
E3 = Y3^2 - d*X3^4 - Z3^4
S(E3)==0
////Algorithm to compute point Addition on Jacobi quartic/////////
R.< d, X1, Y1, X2, Y2, Z1, Z2 > = QQ[]
E1= Y1^2-d*X1^4- Z1^4;
E2= Y2^2-d*X2^4- Z2^4;
S=R.quo([E1, E2])
U1=X1^2

V1=Z1^2

U2=X2^2

V2=Z2^2

U=Y1+V1

V=Y2+V2

RR=Z2*X1

SS=Z1*X2

A=SS-RR

A=A*V;
```

```
A=A*U;

U=U2*U;

V=U1*V;

B=RR*V-SS*U;

D=X1*X2;

E=d*D^2;

D=D*(U-V);

X3=(RR+SS)*(RR-SS);

W1=X1*Z1;

W2=X2*Z2;

Z3=W1*Y2-W2*Y1;

U=Y1*Y2;

V=Z1*Z2;

V=V^2+E;

E=(RR-SS)^2;

U3=X3^2;

V3=Z3^2;

Y3=E*(U+V)-V3
```

```
E3 = Y3^2 - d*X3^4 - Z3^4

S(E3)==0

////// Algorithm to compute point Doubling on Jacobi quartic//////////
R.<d, X2, Y2, Z2> = QQ[]
E2= Y2^2-d*X2^4- Z2^4
S=R.quo([E2])
U2=X2^2;

V2=Z2^2;

U=U2^2;

V=V2^2;

Z3=V-d*U;

E=X2*Z2;

D=2*U2*E;

A=Y2*(Y2+V2);

B=-U2*(Y2+2*V2);

X3=2*E*Y2;

V3=Z3^2;

Y3=2*V-Z3;

Y3=2*Y3^2-V3;

U3=X3^2;
E3 = Y3^2 - d*X3^4 - Z3^4
```

```
S(E3)==0
```

.3 Implementation of the Tate pairing on the Jacobi quartic

```
 //////Parameters
p:=726011672004446604951703464791789328991217313
776602768811505320697581567547878422987036476401963225900 69;
r:=272056320000471307161600306182614014808404525 1
770767719348284547681 7 ;
a:=363005836002223302475851732395894664495608656888 30
138440575266034879078377393921149351823820098161295035;
d:=-a/4;
Fp:=FiniteField(p);
EW:=EllipticCurve([Fp!(a),Fp!0]);
 Fp2<s3>:=ExtensionField<Fp,x|x^2-2>;
  Fp8<W>:=ExtensionField<Fp2,y|y^4-s3>;
EWt:=EllipticCurve([Fp2!(a*s3),Fp2!0]);  /////Twist of EW
//////////////Searching for P of order r on weiertrass////
#EW mod r;   ///// r divides #ElW
u:= #EW /r;
u:=26686080000023115467040000500565104090;
PW:=u*Random(EW);  /////P1 is  point of order r
//////////////Searching of Q of order r  in Weiertrass///////////
#EWt mod r;
 RR:=Random(EWt);
 c:=#EWt/r;
 c:=193744055600612045543444325081021560534457304444
899862776433094111313706912945965421763322 7
      587989498246372460564865343301398950296005788884 66;
QW:=c*RR;
///////////An integer to test bilinearity///////
m:=23;
```

```
Weierstrasstojacobi:=function(PW);
//transform an affine point on the weierstrass form into a
//extended projective  point on the Jacobi form
X1:=2*PW[1];
Y1:=2*PW[1]^3-PW[2]^2;
Z1:=PW[2];
U1:=X1^2 ;
V1:=Z1^2;
return[X1,Y1,Z1,U1,V1];
end function;

PW23:=23*PW;
QW23:=23*QW;
P:= Weierstrasstojacobi(PW);
P23:=Weierstrasstojacobi(PW23);
QJ:=Weierstrasstojacobi(QW);
QJ23:=Weierstrasstojacobi(QW23);
Q:=[QJ[1]/QW[2],QJ[2]/QW[2]^2];
Q23:=[QJ23[1]/QW23[2],QJ23[2]/QW23[2]^2];

Doubling:=function (R, Q);
///Doubling step in Miller Algorithm R (in projective) is the point to be double,
// and S(in affine)  is the point where Tate will be apply(the fixed point)
// given a point Q of order r in E(Fp8) and a 3-uple P(X,Y,Z) in Fp,
// this function computes 2P(X3,Y3,Z3) and the function h_{R,R}(Q)
U:=R[4]^2;
V:=R[5]^2;
Z3:=V-d*U;
E:=R[1]*R[3];
D:=2*R[4]*E;
A:=R[2]*(R[2]+R[5]);
B:=-R[4]*(R[2]+2*R[5]);
X3:=2*E*R[2];
V3:=Z3^2;
Y3:=2*V-Z3;
```

```
Y3:=2*Y3^2-V3;
U3:=X3^2;
M:=(Q[2]+1) / (Q[1]^3*W^4);
N:=(Q[2]+1) / (Q[1]^2*W^4);
H:=A+D*M*W+B*N*W^2;
DBL:=[X3,Y3,Z3,U3,V3, H];
return DBL;
end function;
Addition:=function(R ,S, Q);
///Addition step in Miller Algorithm R,S (in projective) is the point
//to be double, and Q (in affine)  is the point where Tate will be
//apply(the fixed point)given a point Q of order r in E(Fp8) and 2
//3-uple R(X1,Y1,Z1) and S(X2,Y2,Z2) in Fp,
// this function computes
//  R+S(X3,Y3,Z3) and the function h_{R,S}(Q)
U:=R[2]+R[5];
V:=S[2]+S[5];
R1:=S[3]*R[1];
S1:=R[3]*S[1];
A:=S1-R1;
A:=A*V;
A:=A*U;
U:=S[4]*U;
V:=R[4]*V;
B:=R1*V-S1*U;
D:=R[1]*S[1];
E:=d*D^2;
D:=D*(U-V);
X3:=(R1+S1)*(R1-S1);
W1:=R[1]*R[3];
W2:=S[1]*S[3];
Z3:=W1*S[2]-W2*R[2];
U:=R[2]*S[2];
V:=R[3]*S[3];
V:=V^2+E;
E:=(R1-S1)^2;
```

```
U3:=X3^2;
V3:=Z3^2;
Y3:=E*(U+V)-V3;
M:=(Q[2]+1) / (Q[1]^3*W^4);
N:=(Q[2]+1) / (Q[1]^2*W^4);
H:=A+D*M*W+B*N*W^2;
ADD:=[X3,Y3,Z3,U3,V3,H];
return ADD;
end function;

CouplageTate:=function(R ,S);
f:=Fp2!1;
T:=R;
i:=Floor(Log(2,r))-1;
si:=Intseq(r,2);
while i ge 0 do
h:=Doubling(T,S);
f:=h[6]*f^2;
T:=[h[1],h[2],h[3],h[4],h[5]];
if si[i+1] eq 1 then
h:=Addition(R ,T,S);
f:=h[6]*f;
T:=[h[1],h[2],h[3],h[4],h[5]];
end if;
i:=i-1;
end while;
f:=f^(((p^8)-1) div r);
return f;
end function;
e1:=CouplageTate(P,Q);
e23:=CouplageTate(P23,Q);
IsZero(e23-e1^23);
e24:=CouplageTate(P,Q23);
IsZero(e24-e1^23);
```

.4 Implementation of Ate pairing

```
 //////Parameters
p:=726011672004446604951703464791789328991217313776602768811505320697581567547878422987036476404019632259006 9;
 r:=27205632000047130716160030618261401480840452517707677193482845476817 ;
a:=3630058360022233024758517323958946644956086568883013844057526603487907837739392114935182382009816129503 5;
 t:=-113356800000147285043200063789391713609209096429146 0;
Tr:=t-1;
d:=-a/4;
Fp:=FiniteField(p);
EW:=EllipticCurve([Fp!(a),Fp!0]);//Elliptic curve in Weierstrass form defined over Fp//
Fp2<s3>:=ExtensionField<Fp,x|x^2-2>;
Fp8<W>:=ExtensionField<Fp2,y|y^4-s3>;
EWt:=EllipticCurve([Fp2!(a*s3),Fp2!0]); ///////The twist of EW defined over Fp2////
EW8:=EllipticCurve([Fp8!(a),Fp8!0]); /////The curve EW defined over Fp8//////////
///Searching for P of order r on Weiertrass such  that the  frobenius is 1////
 #EW mod r;  //////The order of EW is exactly divisible by r////
 u:= #EW /r;
u:=266860800000231154670400050056510 4090;
P1:=u*Random(EW);    //////P is a point of order r on EW///////
//Point QR of order r on E(Fp8) such that \pi(QR)=p*QR//////////
RR:=Random(EWt);
yy:=#EWt /r;
yy:=193744055600612045543444325081021560534457304444899862776433094111313706912945965
    42176332275879894982463724605648653433013989502960057888846 6;
QRR:=yy*RR;
//////QRR is a point of order r and we send it to EW on Fp8 to apply the Frobenius ///
x1:=QRR[1]*W^(-2);
y1:=QRR[2]*W^(-3);
// (x1,y1) is a point of EW8 defined on Fp8 and we take the frobenius////
x:=x1^p;
y:=y1^p;
D1:=EW8![x,y];
```

```
E1:=EW8![x1,y1];
QR:=D1-E1;  /////// QR satisfies \pi(QR)=p*QR
EW8![QR[1]^p,QR[2]^p]-p*QR;

Weierstrasstojacobi:=function(QR);
//transform an affine point on the weierstrass form
////into a extended projective  point on the Jacobi form
X1:=2*QR[1]/QR[2];
Y1:=(2*QR[1]^3-QR[2]^2)/QR[2]^2;
Z1:=1;
U1:=X1^2 ;
V1:=Z1^2;
return[X1,Y1,Z1,U1,V1];
end function;
////We consider two multiple of P1 and QR to verify bilinearity later //////
P2:=23*P1;
QR1:=23*QR;

//////////////////////The points to be used for Ate pairing computation
Q:=Weierstrasstojacobi(QR);
P:=Weierstrasstojacobi(P1);
Q23:=Weierstrasstojacobi(QR1);
P23:=Weierstrasstojacobi(P2);

Doubling:=function (R, K);
/////Doubling step in Miller Algorithm R (in projective) is the
/////point to be double, and K(in affine)  is the point where Ate
// will be apply(the fixed point)
// given a point K of order r in E(Fp) and a 3-uple (X,Y,Z) in Fp2
// such that (Xw,Y,Z) is a point  in E(Fp8), this function computes
//  (X3,Y3,Z3) sucht that (X3w,Y3,Z3) is its double
// and the function h_{R,R}
U:=R[4]^2;
V:=R[5]^2;
Z3:=V-d*W^4*U;
E:=R[1]*R[3];
```

```
D:=2*R[4]*E;
A:=R[2]*(R[2]+R[5]);
B:=-R[4]*(R[2]+2*R[5]);
X3:=2*E*R[2];
V3:=Z3^2;
Y3:=2*V-Z3;
Y3:=2*Y3^2-V3;
U3:=X3^2;
M:=W^4*(K[2]+1) / (K[1]^3);
N:=(K[2]+1) / (K[1]^2);
H:=M*D+A*W+ B*N*W^3;
return [X3,Y3,Z3,U3,V3,H];
end function;

Addition:=function(R ,S, K);//// R and S are the point to
//////add and K is the point where the pairing is evaluated
// given a point K of order r in E(Fp) and  2 3-uple (X1,Y1,Z1),(X2,Y2,Z2) in Fp2
// such that (Xiw,Yi,Zi) is a point  in E(Fp8), this function computes
//  (X3,Y3,Z3) sucht that (X3w,Y3,Z3) is their sum
// and the function h_{R,S}
U:=R[2]+R[5];
V:=S[2]+S[5];
R1:=S[3]*R[1];
S1:=R[3]*S[1];
A:=S1-R1;
A:=A*V;
A:=A*U;
U:=S[4]*U;
V:=R[4]*V;
B:=R1*V-S1*U;
D:=R[1]*S[1];
E:=d*W^4*D^2;
D:=D*(U-V);
X3:=(R1+S1)*(R1-S1);
W1:=R[1]*R[3];
W2:=S[1]*S[3];
```

```
Z3:=W1*S[2]-W2*R[2];
U:=R[2]*S[2];
V:=R[3]*S[3];
V:=V^2+E;
E:=(R1-S1)^2;
U3:=X3^2;
V3:=Z3^2;
Y3:=E*(U+V)-V3;
M:=(K[2]+1) / (K[1]^3);
N:=(K[2]+1) / (K[1]^2);
H:=M*D*W^4 + A*W+ B*N*W^3;
return[X3,Y3,Z3,U3,V3,H];
end function;
///l:=Addition(Q,Q23,P);
///IsZero(l[2]^2-d*W^4*l[1]^4-l[3]^4);
j2w:=function(P);
//transform an affine point on the jacobi form to the weierstrass form
x:=2*(P[2]+1)/P[1]^2;
 y:=4*(P[2]+1)/P[1]^3;
T:=[x,y];
return T;
end function;
hhfunction:=function(n1,n2,QQ,PP,EW8);////Given two integers n1 and n2,
/// two points QQ and P, hhfunction computes the function h_{n1Q, n2Q}(P)
xQQ:=QQ[1]*W;
yQQ:=QQ[2];
QQ:=[xQQ,yQQ];
QQQ1:=j2w(QQ);
QQ1:= Weierstrasstojacobi(n1*EW8![QQQ1[1],QQQ1[2]]);
QQ2:=Weierstrasstojacobi(n2*EW8![QQQ1[1],QQQ1[2]]);
X1:=QQ1[1]/W;  Y1:=QQ1[2];  Z1:=QQ1[3];
X2:=QQ2[1]/W;  Y2:=QQ2[2];  Z2:=QQ2[3];
if n1 eq n2 then
A:=Y1*(Y1+Z1^2);
B:=-X1^2*(Y1+2*Z1^2);
D:=2*X1^3*Z1;
```

```
H:=(PP[2]+1)/PP[1]^3*D*W^4+ B*(PP[2]+1)/PP[1]^2*W^3 +A*W;
else
A:=(Y1+Z1^2)*(Y2+1)*(Z1*X2-X1);
B:=X1^3*(Y2+1)-X2^3*Z1*(Y1+Z1^2);
D:=X1*X2*(-X1^2*(Y2+1)+X2^2*(Y1+Z1^2));
H:=(PP[2]+1)/PP[1]^3*D*W^4+B*(PP[2]+1)/PP[1]^2*W^3+A*W;
end if;
return H;
end function;
Ate:=function(Q ,S);
f:=1;
////S is given in affine coordinates, the point where we evaluate the Ate
////Q is given in the form (xQ*W,yQ,1,xQ^2*W^2,1)
xQ:=Q[1]/W;
yQ:=Q[2];
zQ:=1;
uQ:=xQ^2;
vQ:=zQ^2;
bin:=Intseq(Abs(Tr),2);
QQ:=[xQ,yQ,1,uQ,vQ];
 T:=QQ;
for i:=#bin-2 to 0 by -1 do
h:=Doubling(T ,S);
T:=[h[1],h[2],h[3],h[4],h[5]];
f:=h[6]*f^2;
if bin[i+1] eq 1 then
h:=Addition(T,QQ ,S);
T:=[h[1],h[2],h[3],h[4],h[5]];
f:=h[6]*f;
end if;
end for;
h1:=hhfunction(Tr,-Tr,QQ,P,EW8);
f:=1/(f*h1)^(Integers()!((p^8-1)/r));
return(f);
end function;
e1:=Ate(Q,P);
```

```
eP23:=Ate(Q,P23);
IsZero(eP23-e1^23);
eQ23:=Ate(Q23,P);
IsZero(eQ23-e1^23);
```

.5 Implementation of the Optimal pairing

```
 //////Parameters
p:=726011672004446604951703464791789328991217317376602768811
05320697581567547878422987036476401963225900 69;
 r:=27205632000047130716160030618261401480840452517707677193482845476817 ;
a:=36300583600222330247585173239589466449560865688830138440575
26603487907837739392114935182382009816129503 5;
 t:=-11335680000014728504320006378939171360920909642914 60;
Tr:=t-1;
d:=-a/4;
x:=24000000000010394;
s1:=(3*x + 1)*p^3;
Fp:=FiniteField(p);
EW:=EllipticCurve([Fp!(a),Fp!0]);//Elliptic curve in Weierstrass form defined over Fp//
Fp2<s3>:=ExtensionField<Fp,x|x^2-2>;
Fp8<W>:=ExtensionField<Fp2,y|y^4-s3>;
EWt:=EllipticCurve([Fp2!(a*s3),Fp2!0]); ///////The twist of EW defined over Fp2////
EW8:=EllipticCurve([Fp8!(a),Fp8!0]); /////The curve EW defined over Fp8//////////
 ///Searching for P of order r on Weiertrass such  that the  frobenius is 1////
 #EW mod r;  //////The order of EW is exactly divisible by r////
 u:= #EW /r;
u:=266860800000231154670400050056510 4090;
P1:=u*Random(EW);    //////P is a point of order r on EW///////
////////////Point QR of order r on E(Fp8) such that \pi(QR)=p*QR/////////////
RR:=Random(EWt);
yy:=#EWt /r;
yy:=193744055600612045543444325081021560534457304444899862776 43
30941113137069129459654217633227587989498246372460564865343301398950296005788884 66;
QRR:=yy*RR;  //////////////QRR is a point of order r and we send
\\ it to EW on Fp8 to apply the Frobenius ////////////////////////////
```

```
x1:=QRR[1]*W^(-2);
y1:=QRR[2]*W^(-3);
///////// (x1,y1) is a point of EW8 defined on Fp8 and we take the frobenius//////
x11:=x1^p;
y11:=y1^p;
D1:=EW8![x11,y11];
E1:=EW8![x1,y1];
QR:=D1-E1;  /////// QR satisfies \pi(QR)=p*QR/////
EW8![QR[1]^p,QR[2]^p]-p*QR;
Weierstrasstojacobi:=function(QR); //transform an affine point on the
\\Weierstrass form into a extended projective  point on the Jacobi form
X1:=2*QR[1]/QR[2];
Y1:=(2*QR[1]^3-QR[2]^2)/QR[2]^2;
Z1:=1;
U1:=X1^2 ;
V1:=Z1^2;
return[X1,Y1,Z1,U1,V1];
end function;
////We consider two multiple of P1 and QR to verify bilinearity later //////
P2:=23*P1;
QR1:=23*QR;
//////////////The points to be used for Ate pairing computation
Q:=Weierstrasstojacobi(QR);
P:=Weierstrasstojacobi(P1);
Q23:=Weierstrasstojacobi(QR1);
P23:=Weierstrasstojacobi(P2);
Doubling:=function (R, K); /////Doubling step in Miller Algorithm R (in projective) is
////point to be double, and K(in affine)  is the point where Ate will be apply(the fixe
// given a point K of order r in E(Fp) and a 3-uple (X,Y,Z) in Fp2
// such that (Xw,Y,Z) is a point  in E(Fp8), this function computes
//  (X3,Y3,Z3) sucht that (X3w,Y3,Z3) is its double
// and the function h_{R,R}
U:=R[4]^2;
V:=R[5]^2;
Z3:=V-d*W^4*U;
E:=R[1]*R[3];
```

```
D:=2*R[4]*E;
A:=R[2]*(R[2]+R[5]);
B:=-R[4]*(R[2]+2*R[5]);
X3:=2*E*R[2];
V3:=Z3^2;
Y3:=2*V-Z3;
Y3:=2*Y3^2-V3;
U3:=X3^2;
M:=W^4*(K[2]+1) / (K[1]^3);
N:=(K[2]+1) / (K[1]^2);
H:=M*D+A*W+ B*N*W^3;
return [X3,Y3,Z3,U3,V3,H];
end function;
Addition:=function(R ,S, K);//// R and S are the point to add
//and K is the point where the pairing is evaluated////////
// given a point K of order r in E(Fp) and  2 3-uple (X1,Y1,Z1), (X2,Y2,Z2) in Fp2
// such that (Xiw,Yi,Zi) is a point  in E(Fp8), this function computes
//  (X3,Y3,Z3) sucht that (X3w,Y3,Z3) is their sum
// and the function h_{R,S}
U:=R[2]+R[5];
V:=S[2]+S[5];
R1:=S[3]*R[1];
S1:=R[3]*S[1];
A:=S1-R1;
A:=A*V;
A:=A*U;
U:=S[4]*U;
V:=R[4]*V;
B:=R1*V-S1*U;
D:=R[1]*S[1];
E:=d*W^4*D^2;
D:=D*(U-V);
X3:=(R1+S1)*(R1-S1);
W1:=R[1]*R[3];
W2:=S[1]*S[3];
Z3:=W1*S[2]-W2*R[2];
```

```
U:=R[2]*S[2];
V:=R[3]*S[3];
V:=V^2+E;
E:=(R1-S1)^2;
U3:=X3^2;
V3:=Z3^2;
Y3:=E*(U+V)-V3;
M:=(K[2]+1) / (K[1]^3);
N:=(K[2]+1) / (K[1]^2);
H:=M*D*W^4 + A*W+ B*N*W^3;
return[X3,Y3,Z3,U3,V3,H];
end function;
///l:=Addition(Q,Q23,P);
///IsZero(l[2]^2-d*W^4*l[1]^4-l[3]^4);
j2w:=function(PP);
//transform an affine point on the jacobi form to the weierstrass form
xpp:=2*(PP[2]+1)/PP[1]^2;
 ypp:=4*(PP[2]+1)/PP[1]^3;
return[xpp,ypp];
end function;
hhfunction:=function(n1,n2,QQ1,QQ2, PP, EW8);
//////Given two integers n1 and n2,
//three points QQ1, QQ2 and P, hhfunction computes the function h_{n1Q, n2Q}(P)
xQQ2:=QQ2[1]*W;
yQQ2:=QQ2[2];
Q2:=[xQQ2,yQQ2];
QQQ12:=j2w(Q2);
QQ2:=Weierstrasstojacobi(n2*EW8![QQQ12[1],QQQ12[2]]);
X2:=QQ2[1]/W;  Y2:=QQ2[2];  Z2:=QQ2[3];
xQQ1:=QQ1[1]*W;
yQQ1:=QQ1[2];
Q1:=[xQQ1,yQQ1];
QQQ11:=j2w(Q1);
QQ1:= Weierstrasstojacobi(n1*EW8![QQQ11[1],QQQ11[2]]);
X1:=QQ1[1]/W;  Y1:=QQ1[2];  Z1:=QQ1[3];
if n1 eq n2  and QQ1 eq QQ2 then
```

```
A:=Y1*(Y1+Z1^2);
B:=-X1^2*(Y1+2*Z1^2);
D:=2*X1^3*Z1;
H:=(PP[2]+1)/PP[1]^3*D*W^4+ B*(PP[2]+1)/PP[1]^2*W^3 +A*W;
else
A:=(Y1+Z1^2)*(Y2+1)*(Z1*X2-X1);
B:=X1^3*(Y2+1)-X2^3*Z1*(Y1+Z1^2);
D:=X1*X2*(-X1^2*(Y2+1)+X2^2*(Y1+Z1^2));
H:=(PP[2]+1)/PP[1]^3*D*W^4+B*(PP[2]+1)/PP[1]^2*W^3+A*W;
end if;
return H;
end function;
Ate:=function(Q ,S);
x:=24000000000010394;
s1:=(3*x + 1)*p^3;
f:=Fp2!1;
////S is given in affine coordinates, the point where we evaluate the Ate
////Q is given in the form (xQ*W,yQ,1,xQ^2*W^2,1)
xQ:=Q[1]/W;
yQ:=Q[2];
zQ:=1;
uQ:=xQ^2;
vQ:=zQ^2;
bin:=Intseq(x ,2);
QQ:=[xQ,yQ,1,uQ,vQ];
 T:=QQ;
for i:=#bin-2 to 0 by -1 do
h:=Doubling(T ,S);
T:=[h[1],h[2],h[3],h[4],h[5]];
f:=h[6]*f^2;
if bin[i+1] eq 1 then
h:=Addition(T,QQ ,S);
T:=[h[1],h[2],h[3],h[4],h[5]];
f:=h[6]*f;
end if;
end for;
```

```
h1:=hhfunction(x,x,QQ,QQ,S,EW8);
h2:=hhfunction(x,2*x,QQ,QQ,S,EW8);
h3:=hhfunction(3*x,1,QQ,QQ,S,EW8);
H1:=(h1*h2*h3)^(p^3);
h4:=hhfunction(s1,x,QQ,QQ,S,EW8);
h5:=hhfunction(s1,0,QQ,QQ,S,EW8);
H2:=h4;
f:=(f^(3*p^3+1)*H1*H2)^(Integers()!((p^8-1)/r));
return(f);
end function;
e1:=Ate(Q,P);
eP23:=Ate(Q,P23);
IsZero(eP23-e1^23);
eQ23:=Ate(Q23,P);
IsZero(eQ23-e1^23);
```

.6 Addition law formulas on level 4 theta model

The Riemann theta formulas give 16 relations that are classified according to j. Remind that $c_0 = a_0, c_2 = a_2/2 = \theta_2(0)/2$ and $a_3 = a_1 = 1$. Let $\mathbb{K}$ be field of characteristic $p \geq 0$ and let $c_0, c_2 \in \mathbb{K}^\star$ and let $E_\lambda : X_0^2 + X_2^2 = \lambda X_1 X_3, X_1^2 + X_3^2 = \lambda X_0 X_2$ be the level 4-theta model defined over field $\mathbb{K}$. The arithmetic (addition and doubling) on E_λ is given by following theta formula :

$$\theta_i(z_1+z_2)\theta_j(z_1-z_2) = \frac{a_k\mathcal{B}(i',j',k',l') - a_{k+2}\mathcal{B}(i',j',k'+2,l')}{a_l}.$$

This formula give 4×4 formulas that give 4 equivalent group laws on E_{λ_1,λ_2}. The 4 group laws formulas are :

$$\begin{aligned}
\theta_i(z_1+z_2)\theta_0(z_1-z_2) &= \frac{a_0\mathcal{B}(i',0,0,i') - a_2\mathcal{B}(i',0,2,i')}{a_i},\\
\theta_i(z_1+z_2)\theta_1(z_1-z_2) &= \frac{a_0\mathcal{B}(i',1,0,i'+1) - a_2\mathcal{B}(i',1,2,i'+1)}{a_{i+1}},\\
\theta_i(z_1+z_2)\theta_2(z_1-z_2) &= \frac{a_0\mathcal{B}(i',2,0,i'+2) - a_2\mathcal{B}(i',2,2,i'+2)}{a_{i+2}},\\
\theta_i(z_1+z_2)\theta_3(z_1-z_2) &= \frac{a_0\mathcal{B}(i',3,0,i'+3) - a_2\mathcal{B}(i',3,2,i'+3)}{a_{i+3}}.
\end{aligned}$$

The first two formulas have been already explained. We deal here by the third and the fourth formulas.

$$③\begin{cases}
\theta_0(z_1+z_2)\theta_2(z_1-z_2) &= \dfrac{c_0\theta_0(z_1)\theta_2(z_1)\theta_1(z_2)\theta_3(z_2) - c_2\Big(\theta_1^2(z_1)\theta_1^2(z_2)+\theta_3^2(z_1)\theta_3^2(z_2)\Big)}{c_2},\\
\theta_1(z_1+z_2)\theta_2(z_1-z_2) &= c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_3(z_2)\Big)\\
&\quad -2c_2\Big(\theta_0(z_1)\theta_3(z_2)\theta_0(z_2)\theta_3(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_1(z_2)\theta_2(z_2)\Big),\\
\theta_2(z_1+z_2)\theta_2(z_1-z_2) &= \dfrac{c_0\Big(\theta_0^2(z_1)\theta_2^2(z_2)+\theta_2^2(z_1)\theta_0^2(z_2)\Big) - 4c_2\theta_1(z_1)\theta_3(z_1)\theta_1(z_2)\theta_3(z_2)}{c_0},\\
\theta_3(z_1+z_2)\theta_2(z_1-z_2) &= c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_2(z_2)\theta_3(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2)\Big)\\
&\quad -2c_2\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_1(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)\Big).
\end{cases}$$

$$④\begin{cases}
\theta_0(z_1+z_2)\theta_3(z_1-z_2) &= c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_2(z_2)\theta_3(z_2)\Big)\\
&\quad -2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_1(z_2)\Big),\\
\theta_1(z_1+z_2)\theta_3(z_1-z_2) &= \dfrac{c_0\Big(\theta_0^2(z_1)\theta_1^2(z_2)+\theta_2^2(z_1)\theta_3^2(z_2)\Big) - 4c_2\theta_1(z_1)\theta_3(z_1)\theta_0(z_2)\theta_2(z_2)}{c_0},\\
\theta_2(z_1+z_2)\theta_3(z_1-z_2) &= c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_1(z_1)\theta_2(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_0(z_2)\theta_3(z_2)\Big)\\
&\quad -2c_2\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_3(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2)\Big),\\
\theta_3(z_1+z_2)\theta_3(z_1-z_2) &= \dfrac{c_0\theta_0(z_1)\theta_2(z_1)\theta_1(z_2)\theta_3(z_2) - c_2\Big(\theta_1^2(z_1)\theta_0^2(z_2)+\theta_3^2(z_1)\theta_2^2(z_2)\Big)}{c_2}.
\end{cases}$$

.7 Sage verification : Addition and doubling of points on Level 4 theta model

This sage script verifies that addition formulas are valid.

```
/////////Addition formulas  and algorithm on the level 4 theta model/////////
R.<c0,c2,X0,X1,X2,X3,Y0,Y1,Y2,Y3> = QQ[]
  lbd = c0^2 + 4*c2^2;
  LB = numerator(lbd -1/(c0*c2))
  E1 = numerator(X0^2 + X2^2 - lbd*X1*X3);
  E2 = numerator(X1^2 + X3^2 - lbd*X0*X2)
  F1 = numerator(Y0^2 + Y2^2 - lbd*Y1*Y3);
  F2 = numerator(Y1^2 + Y3^2 - lbd*Y0*Y2)
  S = R.quo([E1,E2,F1,F2,LB])
```

```
  Z0 = (X0^2*Y0^2 + X2^2*Y2^2) - 4*(c2/c0)*X1*X3*Y1*Y3
  Z1 = c0*(X0*X1*Y0*Y1 + X2*X3*Y2*Y3) - 2*c2*(X2*X3*Y0*Y1 + X0*X1*Y2*Y3)
  Z2 = (X1^2*Y1^2 + X3^2*Y3^2) - 4*(c2/c0)*X0*Y0*X2*Y2
  Z3 = c0*(X0*X3*Y0*Y3 + X1*X2*Y1*Y2) - 2*c2*(X0*X3*Y1*Y2 + X1*X2*Y0*Y3)
  G1 = Z0^2 + Z2^2 - lbd*Z1*Z3; G2 = Z1^2 + Z3^2 - lbd*Z0*Z2
  S(numerator(G1)) == 0; S(numerator(G2)) == 0
U1=X0*X1; V1=X2*X3; U2=Y0*Y1; V2=Y2*Y3
A=X0*Y0; B=X1*Y1; C= X2*Y2; D=X3*Y3; E=A^2 ; F=B^2
 G=C^2; H=D^2; Z0=E+G+((2*c2)/c0)*((B-D)^2-F-H);
Z2=F+H+((2*c2)/c0)*((A-C)^2-E-G); I=(1/2)*((A+B)^2-E-F);
J=(1/2)*((C+D)^2-G-H); K=(U1+V1)*(U2+V2)-I-J; L=(A+C)*(B+D)-I-J;
Z1=c0*(I+J)-2*c2*K;
E=(X0+X2)*(X3+X1)-U1-V1;  F=(Y0+Y2)*(Y3+Y1)-U2-V2; G=E*F-L;
Z3=c0*L-2*c2*G; U3=Z0*Z1; V3=Z2*Z3
G1 = Z0^2 + Z2^2 - lbd*Z1*Z3; G2 = Z1^2 + Z3^2 - lbd*Z0*Z2
 S(numerator(G1)) == 0; S(numerator(G2)) == 0

////////////  Algorithm of Addition of points : Binary Fields////////
R.<c0,c2,X0,X1,X2,X3,Y0,Y1,Y2,Y3> = GF(2)[]
  lbd = c0^2 + 4*c2^2;
  LB = numerator(lbd -1/(c0*c2))
  E1 = numerator(X0^2 + X2^2 - lbd*X1*X3);
  E2 = numerator(X1^2 + X3^2 - lbd*X0*X2)
  F1 = numerator(Y0^2 + Y2^2 - lbd*Y1*Y3);
  F2 = numerator(Y1^2 + Y3^2 - lbd*Y0*Y2)
  S = R.quo([E1,E2,F1,F2,LB])
A=X0*Y0; B=X1*Y1;  C=X2*Y2; D=X3*Y3; Z0=(A+C)^2; Z2=(B+D)^2;
Z1=c0*(A*B+C*D) ;  Z3 =c0*(A+C)*(B+D)-Z1
G1 = Z0^2 + Z2^2 - lbd*Z1*Z3; G2 = Z1^2 + Z3^2 - lbd*Z0*Z2
 S(numerator(G1)) == 0; S(numerator(G2)) == 0

/////Difference of points P-Q on level 4 theta model//////////////
R.<c0,c2,X0,X1,X2,X3,Y0,Y1,Y2,Y3> = QQ[]
  lbd = c0^2 + 4*c2^2;
  LB = numerator(lbd -1/(c0*c2))
  E1 = numerator(X0^2 + X2^2 - lbd*X1*X3);
```

```
  E2 = numerator(X1^2 + X3^2 - lbd*X0*X2)
  F1 = numerator(Y0^2 + Y2^2 - lbd*Y1*Y3);
  F2 = numerator(Y1^2 + Y3^2 - lbd*Y0*Y2)
  S = R.quo([E1,E2,F1,F2,LB])
T0 = (X0^2*Y0^2 + X2^2*Y2^2) - 4*(c2/c0)*X1*X3*Y1*Y3
T1 = c0*(X0*X1*Y0*Y3 + X2*X3*Y2*Y1) - 2*c2*(X2*X3*Y0*Y3 + X0*X1*Y2*Y1)
T2 = (X1^2*Y3^2 + X3^2*Y1^2) - 4*(c2/c0)*X0*X2*Y0*Y2
T3 = c0*(X0*X3*Y0*Y1 + X1*X2*Y3*Y2) - 2*c2*(X0*X3*Y3*Y2 + X1*X2*Y0*Y1)
Q1 = T0^2 + T2^2 - lbd*T1*T3; Q2 = T1^2 + T3^2 - lbd*T0*T2
  S(numerator(Q1)) == 0; S(numerator(Q2)) == 0
/////////////// Doubling on level 4 theta model///////
R.<c0,c2,X0,X1,X2,X3,Y0,Y1,Y2,Y3> = QQ[]
  lbd = c0^2 + 4*c2^2;
  LB = numerator(lbd -1/(c0*c2))
  E1 = numerator(X0^2 + X2^2 - lbd*X1*X3);
  E2 = numerator(X1^2 + X3^2 - lbd*X0*X2)
  F1 = numerator(Y0^2 + Y2^2 - lbd*Y1*Y3);
  F2 = numerator(Y1^2 + Y3^2 - lbd*Y0*Y2)
  S = R.quo([E1,E2,F1,F2,LB])
U0=X0^4 + X2^4 - 4*(c2/c0)*X1^2*X3^2
U1=c0*(X0^2*X1^2 + X2^2*X3^2) - 4*c2*X0*X1*X2*X3
U2=X1^4 + X3^4 - 4*(c2/c0)*X0^2*X2^2
U3=c0*(X0^2*X3^2 + X1^2*X2^2) - 4*c2*X0*X1*X2*X3
R1 = U0^2 + U2^2 - lbd*U1*U3; R2 = U1^2 + U3^2 - lbd*U0*U2
  S(numerator(R1)) == 0; S(numerator(R2)) == 0
///////// Doubling algorithm: Odd characteristic//////////
R.<c0,c2,X0,X1,X2,X3,Y0,Y1,Y2,Y3> = QQ[]
  lbd = c0^2 + 4*c2^2;
  LB = numerator(lbd -1/(c0*c2))
  E1 = numerator(X0^2 + X2^2 - lbd*X1*X3);
  E2 = numerator(X1^2 + X3^2 - lbd*X0*X2)
  F1 = numerator(Y0^2 + Y2^2 - lbd*Y1*Y3);
  F2 = numerator(Y1^2 + Y3^2 - lbd*Y0*Y2)
  S = R.quo([E1,E2,F1,F2,LB])
U1=X0*X1; V1=X2*X3; A=X0*X2; B=X1*X3; C=A^2; D=B^2;
Z0=(lbd^2-4*c2^2*lbd)*D-2*C;
```

```
Z2=(lbd^2-4*c2^2*lbd)*C-2*D; E=U1*V1; F=(U1+V1)^2-2*E;
Z1=c0*F-4*c2*E;
Z3=c0*(((X0+X1)*(X3+X2)-A-B)^2-2*E)-4*c2*E ; U3=Z0*Z1; V3=Z2*Z3
G1 = Z0^2 + Z2^2 - lbd*Z1*Z3; G2 = Z1^2 + Z3^2 - lbd*Z0*Z2
 S(numerator(G1)) == 0; S(numerator(G2)) == 0
////////////// Doubling algorithm: Binary Fields///////////////
R.<c0,c2,X0,X1,X2,X3,Y0,Y1,Y2,Y3> = GF(2)[]
  lbd = c0^2 + 4*c2^2;
  LB = numerator(lbd -1/(c0*c2))
  E1 = numerator(X0^2 + X2^2 - lbd*X1*X3);
  E2 = numerator(X1^2 + X3^2 - lbd*X0*X2)
  F1 = numerator(Y0^2 + Y2^2 - lbd*Y1*Y3);
  F2 = numerator(Y1^2 + Y3^2 - lbd*Y0*Y2)
  S = R.quo([E1,E2,F1,F2,LB])
A=X0^2; B=X1^2; C=X2^2; D=X3^2; Z0=(A+C)^2; Z2=(B+D)^2;
Z1=c0*(A*B+C*D); Z3=c0*(A+C)*(B+D)-Z1
G1 = Z0^2 + Z2^2 - lbd*Z1*Z3; G2 = Z1^2 + Z3^2 - lbd*Z0*Z2
S(numerator(G1)) == 0; S(numerator(G2)) == 0
```

.8 Sage verification : Differential addition

This sage script verifies that differential addition formulas are valid.

```
////////////// Differential addition on level 4 theta model///////////////
R.<c0,c2,X0,X1,X2,X3,Y0,Y1,Y2,Y3> = QQ[]
  lbd = c0^2 + 4*c2^2;
  LB = numerator(lbd -1/(c0*c2))
  E1 = numerator(X0^2 + X2^2 - lbd*X1*X3);
  E2 = numerator(X1^2 + X3^2 - lbd*X0*X2)
  F1 = numerator(Y0^2 + Y2^2 - lbd*Y1*Y3);
  F2 = numerator(Y1^2 + Y3^2 - lbd*Y0*Y2)
 S = R.quo([E1,E2,F1,F2,LB])
T0 = (X0^2*Y0^2 + X2^2*Y2^2) - 4*(c2/c0)*X1*X3*Y1*Y3
T1 = c0*(X0*X1*Y0*Y3 + X2*X3*Y2*Y1) - 2*c2*(X2*X3*Y0*Y3 + X0*X1*Y2*Y1)
T2 = (X1^2*Y3^2 + X3^2*Y1^2) - 4*(c2/c0)*X0*X2*Y0*Y2
T3 = c0*(X0*X3*Y0*Y1 + X1*X2*Y3*Y2) - 2*c2*(X0*X3*Y3*Y2 + X1*X2*Y0*Y1)
```

```
Z0=T0
Z2= ((c0^2 -4*c2^2)/(c0*c2))*X0*Y0*X2*Y2- T2
 Z1 = c0*(X0*X1*Y0*Y1 + X2*X3*Y2*Y3) - 2*c2*(X2*X3*Y0*Y1 + X0*X1*Y2*Y3)
 Z3 = c0*(X0*X3*Y0*Y3 + X1*X2*Y1*Y2) - 2*c2*(X0*X3*Y1*Y2 + X1*X2*Y0*Y3)
 G1 = Z0^2 + Z2^2 - lbd*Z1*Z3; G2 = Z1^2 + Z3^2 - lbd*Z0*Z2
U0= (1-4*c0*c2^3)*(X0^2 + X2^2)^2 - 2*X0^2*X2^2
U2=((1-4*c0*c2^3)/(c0^2*c2^2))*X0^2*X2^2 - 2*c2^2*c0^2* (X0^2 + X2^2)^2
U1=c0*(X0^2*X1^2 + X2^2*X3^2) - 4*c2*X0*X1*X2*X3
U3=c0*(X0^2*X3^2 + X1^2*X2^2) - 4*c2*X0*X1*X2*X3
R1 = U0^2 + U2^2 - lbd*U1*U3; R2 = U1^2 + U3^2 - lbd*U0*U2
  S(numerator(R1)) == 0; S(numerator(R2)) == 0
  S(numerator(G1)) == 0; S(numerator(G2)) == 0
```

VU :

Le Directeur de Thèse
(Nom et Prénom)

VU :

Le Responsable de l'École Doctorale

VU pour autorisation de soutenance

Rennes, le

Le Président de l'Université de Rennes 1

Guy CATHELINEAU

VU après soutenance pour autorisation de publication :

Le Président de Jury,
(Nom et Prénom)

RESUME

Alors qu'initialement utilisés pour résoudre le Problème du Logarithme Discret (DLP) dans le groupe de points d'une courbe elliptique [8], [5], les couplages sont très à la mode en cryptographie ces années car ils permettent de construire de nouveaux protocoles cryptographiques [3], [7], [1]. Cependant, le calcul efficace du couplage dépend de l'arithmétique du modèle de courbe elliptique choisi et du corps sur lequel cette courbe est définie. Dans cette thèse, nous calculons le couplage sur deux modèles de Jacobi de courbes elliptiques puis nous introduisons et étudions l'arithmétique d'un nouveau modèle d'Ewards de courbe elliptiques défini en toutes caractéristiques. Plus précisément, Nous utilisons l'interprétation géométrique de la loi de groupe sur l'intersection des quadriques de Jacobi pour obtenir pour la première fois dans la littérature, les formules explicites de la fonction de Miller pour le calcul du couplage de Tate sur cette courbe. Pour un calcul de couplage avec un degré de plongement pair, nous définissons la tordue quadratique pour obtenir des étapes de doublement et d'addition efficaces dans l'algorithme de Miller. Ensuite nous utilisons un isomorphisme entre la quartique spéciale de Jacobi $E_d : Y^2 = dX^4 + Z^4$ et le modèle de Weierstrass pour obtenir la fonction de Miller nécessaire au calcul du couplage de Tate. Pour un degré de plongement divisible par 4, nous définissons la tordue d'ordre 4 de cette courbe pour obtenir un résultat meilleur du calcul du couplage de Tate par rapport aux courbes elliptiques sous forme de Weierstrass. Notre résultat améliore en même temps les derniers résultats obtenus sur cette courbe [9]. Ce résultat est donc le meilleur connu à ce jour, à notre connaissance, pour le calcul du couplage de Tate sur les courbes possédant des tordues d'ordre 4. En 2006, Hess et al. introduisent dans [6] le couplage Ate, qui est une version améliorée du couplage de Tate. Nous calculons ce couplage et ses variantes sur la même quartique. Nous y obtenons encore des résultats meilleurs. Notre troisième contribution est l'introduction d'un nouveau modèle d'Edwards de courbe elliptique d'équation $1 + x^2 + y^2 + x^2y^2 = \lambda xy$. Ce modèle est ordinaire sur les corps de caractéristique 2 et nous montrons qu'il est birationnellement équivalent au modèle original d'Edwards $x^2 + y^2 = c^2(1 + x^2y^2)$ [4] en caracteristique différente de 2. Pour ce fait, nous utilisons la théorie des fonctions thêta et un modèle intermédiaire que nous appelons modèle thêta de niveau 4. Nous utilisons les relations de Riemann des fonctions thêta pour étudier l'arithmétique de ces deux courbes. Nous obtenons d'une part une loi de groupe complète, unifiée et en particulier compétitive en caractéristique 2 et d'autre part nous présentons les meilleures formules d'addition différentielle sur le modèle thêta de niveau 4.

ABSTRACT

While first used to solve the Discrete Logarithm Problem (DLP) in the group of points of elliptic curves [8], [5], bilinear pairings are now useful to construct many public key protocols [3]. The efficiency of pairings computation depends on the arithmetic of the model chosen for the elliptic curve and of the base field where the curve is defined. In this thesis, we compute and implement pairings on elliptic curves of Jacobi forms and we study the arithmetic of a new Edwards model for elliptic curves defined over any finite field. More precisely, We use the geometric interpretation of the group law of Jacobi intersection curves to obtain the first explicit formulas for the Miller function in Tate pairing computation in this case. For pairing computation with even embedding degree, we define and use the quadratic twist of this curve to obtain efficient formulas in the doubling and addition stages in Miller's algorithm. Moreover, for pairing computation with embedding degree divisible by 4 on the special Jacobi quartic elliptic curve $E_d : Y^2 = dX^4 + Z^4$, we define and use its quartic twist to obtain a best result with respect to Weierstrass curves [2]. Our result is at the same time an improvement of a result recently obtained on this curve [9], and is therefore, to our knowledge, the best result to date on Tate pairing computation among all curves with quartic twists. In 2006, Hess et al. introduced the concept of Ate pairing [6] which is an improving version of the Tate pairing. We extend the computation of this pairing and its variations to the curve E_d. Again our theoretical results show that this curve offers the best performances comparatively to other curves with quartic twists, especially Weiertrass curves. As a third contribution, we introduce a new Edwards model for elliptic curves with equation $1 + x^2 + y^2 + x^2y^2 = \lambda xy$. This model is ordinary over binary fields and we show that it is birationally equivalent to the well known Edwards model $x^2 + y^2 = c^2(1 + x^2y^2)$ of [4] over non-binary fields. For this, we use the theory of theta functions to obtain an intermediate model that we call the level 4 theta model. We study the arithmetic of these curves, using Riemann relations of theta functions. The group laws are complete, unified, efficient and are particularly competitive in characteristic 2. Our formulas for differential addition on the level four theta model over binary fields are the best to date among well known models of elliptic curves.